la République Tunisienne
Ministère de la Famille, de la Femme,
de l'Enfance et des Personnes âgées

Diagnostic institutionnel pour la prévention et la réponse à la violence à l'égard des enfants en ligne

USAID
DU PEUPLE AMERICAIN

unicef
pour chaque enfant

Table des matières

I. Remerciements

Ce rapport a été rédigé par Hanen Keskes, Alexander Martin, Wissem Heni (Resolve Consulting) et Patrick Burton (Centre pour la justice et la prévention du crime). L'étude a été réalisée grâce au soutien de nombreuses personnes, dont le ministère de la Famille, de la Femme, de l'Enfance et des Seniors (MFFES)., qui a commandé le travail, avec le soutien du bureau de l'UNICEF en Tunisie.

En particulier, les auteurs tiennent à adresser leurs remerciements à Antoine Deliege, Chadi Rabhi et Rabeb Ayari (UNICEF Tunisie, Protection de l'Enfance), et à M. Samir Ben Meriem, Mme Jamila Bettaieb,M. Ali Belhadi, Rami Ben Sallah et Nejib Tout du MFFES et M. Lotfi Belazi, directeur général du Centre national de l'informatique pour l'enfant (CNIPE).

Les auteurs tiennent aussi à remercier les nombreux responsables, représentants de la société civile et toutes autres parties prenantes qui ont participé à l'étude et donné si généreusement de leur temps, ainsi que le comité de pilotage du projet.

L'équipe a une énorme dette de gratitude envers les enfants, les parents et les instituteurs qui ont donné de leur temps pour parler si ouvertement et honnêtement pendant les discussions de groupe.

L'étude a été financée par l'UNICEF Tunisie à travers des fonds du comité national français d'UNICEF.

II. Acronymes

ATI	Agence Tunisienne d'Internet
BEC	Les bureaux d'écoute et de conseil
CEC	Les cellules d'écoute et de conseil
CG	Commentaire général (n° 25 sur les droits de l'enfant dans l'environnement numérique)
CNIPE	Centre National de l'informatique pour l'Enfant
CRDE	Convention relative aux droits de l'enfant
DGPE	Délègue Général à la protection de l'enfance
DPE	Délégué à la protection de l'enfance
EASEL	Exploitation et abus sexuels d'enfants en ligne
ECVS	Education aux compétences de vie et à la citoyenneté
EPPC	Entretien avec les parties Prenantes Clés
GD	Groupe de discussion
INTLP	Instance Nationale de Lutte contre la Traite des Personnes
FAI	Fournisseur d'accès à Internet
MESE	Matériel d'exploitation sexuelle d'enfants
MFFES	Ministère de la Famille, de la Femme, de l'Enfance et des Seniors
MRN	Modèle de Réponse Nationale
PAN	Plan d'Action National
PE	Protection de l'enfance
PELE	Protection en ligne des enfants
PPIPPE	Politique Publique Intégrée de Prevention et de Protection de l'Enfance
TIC	Technologies de l'information et de la communication
TSA	Troubles du Spectre Autistique
VCE	Violence contre les enfants

III. Glossaire

Terme	Définition
Assistance téléphonique	Les lignes d'assistance fournissant des conseils et une assistance confidentielle aux appelants, agissant souvent comme points de référence vers d'autres prestataires de services.
Cyberintimidation (Cyberbullying) Adapté du Park, M. S.-A., Golden, K. J., Vizcaino-Vickers, S., Jidong, D., & Raj, S. (2021). Sociocultural values, attitudes and risk factors associated with adolescent cyberbullying in East Asia: A systematic review. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 15(1), Article 5.	Modèle intentionnel de comportement blessant qui implique généralement des éléments de déséquilibre de pouvoir, infligés par l'utilisation d'ordinateurs, de téléphones portables et d'autres appareils numériques. La cyberintimidation peut chevaucher l'intimidation hors ligne.
Données personnelles Le Fonds des Nations Unies pour l'enfance, 'Child Protection in Digital Education: Technical Note', UNICEF, New York, janvier 2023 ; adapté de Day, E. (2021). Governance of data for children's learning in UK state schools. Digital Futures Commission, 5Rights Foundation.	Toute information relative à un enfant individuel qui permet de l'identifier directement à partir de cette information ou indirectement lorsque l'information est combinée avec d'autres informations.
Éducation numérique Adapté du Fonds des Nations Unies pour l'enfance, 'La protection de l'enfance dans l'éducation numérique : Note technique', UNICEF, New York, janvier 2023 ; adapté de Day, E. (2021). Gouvernance des données pour l'apprentissage des enfants dans les écoles publiques du Royaume-Uni. Commission de l'avenir numérique, Fondation 5Rights.	Tout processus d'enseignement ou d'apprentissage qui implique l'utilisation de la technologie numérique, y compris les formats en ligne et hors ligne, en utilisant des approches à distance, en personne ou hybrides.

Edtech Le Fonds des Nations Unies pour l'enfance, 'La protection de l'enfance dans l'éducation numérique : Note technique', UNICEF, New York, janvier 2023 ; adapté de Day, E. (2021). Gouvernance des données pour l'apprentissage des enfants dans les écoles publiques du Royaume-Uni. Commission de l'avenir numérique, Fondation 5Rights.	La technologie de l'éducation (EdTech) fait référence à la pratique consistant à utiliser la technologie pour soutenir l'enseignement et la gestion quotidienne efficace des établissements d'enseignement. Elle comprend du matériel (tel que des tablettes, des ordinateurs portables ou d'autres appareils numériques) et des ressources numériques (telles que des plateformes et du contenu), des logiciels et des services qui facilitent l'enseignement, répondent à des besoins spécifiques et facilitent le fonctionnement quotidien des établissements d'enseignement.
Enfant Article 1, Convention relative aux droits de l'enfant (CRC), 1989 Article 3, Code de la Protection de l'Enfant	Tout être humain âgé de moins de dix-huit ans sauf en vertu de la loi applicable à l'enfant, la majorité est atteinte plus tôt. D'après l'article 3 du Code de la Protection de l'Enfant « est enfant, aux effets du présent code, toute personne humaine âgée de moins de dix-huit ans et qui n'a pas encore atteint l'âge de la majorité par dispositions spéciales »
Exploitation et abus sexuels d'enfants Article 18, Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (Convention de Lanzarote) ECPAT. Lignes directrices terminologiques pour la protection des enfants contre l'exploitation et les abus sexuels. Adopté par le groupe de travail interagences à Luxembourg, le 28 janvier 2016 Voir aussi : Comité des droits de l'enfant, Lignes directrices concernant la mise en œuvre du Protocole facultatif à la Convention relative aux droits de l'enfant concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants, CRC/C/156, 10 septembre 2019.	**L'abus sexuel d'enfant comprend le faite de:** (a) Se livrer à des activités sexuelles avec un enfant qui, conformément aux dispositions pertinentes de la législation nationale, n'a pas atteint l'âge légal pour les activités sexuelles (cela ne s'applique pas aux activités sexuelles consensuelles entre mineurs), et (b) Se livrer à des activités sexuelles avec un enfant en recourant à la coercition, à la force ou à des menaces ; ou un abus est fait d'une position reconnue de confiance, d'autorité ou d'influence sur l'enfant, y compris au sein de la famille ; ou abus est fait d'une situation particulièrement vulnérable de l'enfant, notamment en raison d'un handicap mental ou physique ou d'une situation de dépendance.

	L'abus sexuel d'un enfant devient une exploitation sexuelle lorsqu'une deuxième partie en profite financièrement, par le biais d'une activité sexuelle impliquant un enfant. Il comprend des actes préjudiciables tels que la sollicitation sexuelle et l'exploitation sexuelle d'un enfant ou d'un adolescent dans la prostitution et, dans la Convention du Conseil de l'Europe, couvre les situations dans lesquelles un enfant ou une autre personne se voit offrir ou promettre de l'argent ou une autre forme de rémunération, de paiement ou de considération en échange de l'engagement de l'enfant dans une activité sexuelle, même si le paiement/ rémunération n'est pas effectué. Bien que les termes soient parfois utilisés de manière interchangeable, ce qui distingue le concept d'exploitation sexuelle d'enfants de celui d'abus sexuel d'enfants est la notion sous-jacente d'échange, financier ou autre.
Abus sexuel basé sur l'image (facilité par la technologie) Adapté de Radford, Lorraine, et al., Action to End Child Abuse and Exploitation: A review of the evidence, UNICEF Child Protection Section, Programme Division, New York, December 2020	La création et/ou la distribution non consensuelle et/ou la menace de distribution d'images privées à caractère sexuel. L'abus sexuel basé sur l'image peut être utilisé pour décrire une gamme d'infractions non consensuelles impliquant la création et la diffusion d'images sexuelles privées, y compris la pornographie de vengeance, l'upskirting, la production de médias deepfake et le cyber-flashing. Cela comprend également le harcèlement sexuel fondé sur l'image, qui fait référence au partage non sollicité d'images sexuelles.
Piratage (hacking) VAW Learning Network (2013). Technology-related Violence Against Women.	Utilisation de la technologie pour « obtenir un accès illégal ou non autorisé à des systèmes ou à des ressources dans le but d'acquérir des informations personnelles, d'altérer ou de modifier des informations, ou de calomnier et de dénigrer, ou de recourir à la violence. »

Harcèlement en ligne et harcèlement sexuel en ligne N. Henry and A. Powell (2018) Technology-facilitated sexual violence: a literature review of empirical research. Trauma, Violence & Abuse, vol. 19, No. 2, pp. 195–208	Contacter, ennuyer, menacer ou effrayer à plusieurs reprises une autre personne, que ce soit par un individu ou un groupe. Le harcèlement sexuel en ligne comprend une attention sexuelle non invitée et une coercition sexuelle.
Industrie technologique UIT Lignes directrices pour l'industrie sur la protection en ligne des enfants, 2020	Le secteur des TIC ou de la technologie couvre un large éventail d'entreprises, y compris, mais sans s'y limiter : (a) Fournisseurs d'accès à Internet (FAI), y compris par le biais de services fixes haut débit fixes ou de services de données cellulaires d'opérateurs de réseaux mobiles : bien que cela reflète généralement les services offerts à plus long terme aux clients abonnés, cela pourrait également être étendu aux entreprises qui fournir des hotspots WI-FI publics gratuits ou payants. (b) Plateformes de réseaux sociaux/messagerie et plateformes de jeux en ligne. (c) Les fabricants de matériel et de logiciels, tels que les fournisseurs d'appareils portables, y compris les téléphones portables, les consoles de jeux, les appareils domestiques basés sur l'assistance vocale, l'Internet des objets et les jouets intelligents connectés à Internet pour les enfants. (d) Entreprises fournissant des médias numériques (créateurs de contenu, fournissant un accès ou hébergeant du contenu). (e) Entreprises fournissant des services de streaming, y compris des flux en direct. (f) Entreprises offrant des services de stockage de fichiers numériques, fournisseurs de services basés sur le cloud.

Ligne d'assistance	Un mécanisme de signalement en ligne dédié pour signaler le matériel Internet suspecté d'être illégal, y compris le matériel d'abus sexuel d'enfants. Une hotline permet au public de signaler de manière anonyme les contenus en ligne qu'ils soupçonnent d'être illégaux. **Une Ligne d'assistance** est distincte d'une **Assistance téléphonique** (voir ci-dessus).
Matériel d'exploitation sexuelle d'enfants Comité des droits de l'enfant, Lignes directrices concernant la mise en œuvre du Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants, CRC/C/156, 10 septembre 2019, para 60	Le matériel d'exploitation sexuelle d'enfants est couvert par l'article 2 du Protocole facultatif à la CDE concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants en tant que « pornographie mettant en scène des enfants », et est défini comme toute représentation, par quelque moyen que ce soit, d'un enfant engagé dans des activités réelles ou des activités sexuelles explicites simulées ou toute représentation des parties sexuelles d'un enfant à des fins principalement sexuelles (art. 2 c)). Le Comité des droits de l'enfant recommande aux États parties, conformément aux évolutions récentes, d'éviter autant que possible le terme « pornographie enfantine » et d'utiliser d'autres termes tels que «l'utilisation d'enfants dans des spectacles et du matériel pornographiques », « matériel d'exploitation sexuelle d'enfants » et « matériel d'exploitation sexuelle d'enfants ».
Prévention Organisation mondiale de la santé (OMS), Rapport mondial sur la violence et la santé, OMS, Genève, 2002.	Suit la définition de l'OMS de la « prévention primaire » : Mettre fin aux abus et à l'exploitation sexuels des enfants avant qu'ils ne surviennent.
Sollicitation (grooming) en ligne d'un enfant à des fins sexuelles Article 23, Convention de Lanzarote	Proposition intentionnelle, par le biais des technologies de l'information et de la communication, d'un adulte pour rencontrer un enfant qui n'a pas atteint l'âge légal pour des activités sexuelles, dans le but de se livrer à des activités sexuelles ou de produire du matériel d'abus sexuel d'enfants.

Violence contre les enfants Article 19, Convention relative aux droits de l'enfant (CRC), 1989	Toutes les formes de violence physique ou mentale, de blessures et d'abus, de négligence ou de traitement négligent, de mauvais traitements ou d'exploitation, y compris la violence émotionnelle et l'abus sexuel.
Violences sexuelles Radford, Lorraine, et al., Action to End Child Abuse and Exploitation: A review of the evidence, UNICEF Child Protection Section, Programme Division, New York, December 2020	Terme générique utilisé ici pour désigner toutes les formes de victimisation sexuelle des femmes adultes et des enfants - abus et exploitation sexuels d'enfants, viols et autres agressions sexuelles, harcèlement sexuel, abus dans la pornographie, prostitution et traite, MGF. Tout acte sexuel, tentative d'obtenir un acte sexuel, commentaires ou avances sexuels non désirés, ou actes de trafic, ou autrement dirigés contre la sexualité d'une personne en utilisant la coercition, par toute personne, quelle que soit sa relation avec la victime, dans n'importe quel contexte, y compris mais ne se limite pas à la maison et au travail.

I. Résumé

1. Contexte

Les technologies de l'information et de la communication (TIC) sont devenues un aspect fondamental de la vie quotidienne des enfants. Bien que l'accès à cette technologie offre de nombreux avantages éducatifs et sociaux aux enfants, elles ont également le potentiel de les exposer à des risques et de leur causer du préjudice. De plus, les risques en ligne peuvent facilement devenir des préjudices hors ligne. Resolve Consulting et le Centre pour la justice et la prévention du crime (CJCP), avec le financement et le soutien de l'UNICEF (Bureau de Tunisie) ont mené ce projet de recherche visant à soutenir le gouvernement tunisien à renforcer sa capacité à prévenir, détecter et faire face aux types de vulnérabilités et de violence contre les enfants dans le monde virtuel. Les résultats seront utilisés pour éclairer l'élaboration d'un plan d'action national (PAN) pour lutter contre la violence en ligne à l'égard des enfants.

2. Méthodologie

Pour évaluer la protection juridique accordée aux enfants en Tunisie, cette recherche a mené une cartographie approfondie du cadre juridique, y compris les lois nationales tunisiennes et les conventions internationales sur la protection de l'enfance signées par le gouvernement tunisien. Cela a été combiné avec une cartographie des structures et mécanismes institutionnels impliqués dans le paysage de la protection en ligne de l'enfant en Tunisie. Afin d'explorer les types de violence en ligne auxquels les enfants tunisiens sont confrontés en plus des réponses et des lacunes existantes, la recherche a collecté des données qualitatives par le biais de groupes de discussions et d'entretiens avec les principales parties prenantes. Celle-ci a évalué les besoins et les capacités des secteurs concernés et a exploré les expériences en ligne des enfants. 17 entretiens ont été menés avec des acteurs gouvernementaux, des ONG internationales, des acteurs judiciaires, de la santé et de la société civile dans le domaine de la protection en ligne des enfants. Pour garantir une approche centrée sur l'enfant, 16 groupes de discussion ont été organisés avec 113 enfants (49 garçons, 64 filles) âgés de 13 à 17 ans dans quatre sites de recherche dans cinq gouvernorats (Grand Tunis (Tunis, Manouba), Jendouba, Gafsa, et Kasserine). Pour corroborer et contraster ces résultats, sept autres groupes de discussion ont été organisés avec des 28 parents et des 22 éducateurs. Ces résultats de recherche qualitative fournissent des comptes rendus détaillés, des perspectives personnelles et des informations importantes sur la vie numérique des enfants en Tunisie. Ces données peuvent éclairer les recommandations et les prochaines étapes pour garantir la réalisation des droits collectifs des enfants en Tunisie et la promotion d'un environnement en ligne sûr.

3. Résultats de recherche

Les groupe de discussions avec les enfants ont révélé qu'ils apprécient les nombreux avantages éducatifs et sociaux qu'offre l'Internet. De plus, l'utilisation d'Internet offre des opportunités de divertissement, de développement personnel et des bénéfices commerciales, en plus d'apporter des avantages pour la santé mentale. Cependant, les mêmes enfants reconnaissent qu'une utilisation excessive d'Internet peut avoir des effets négatifs sur la santé physique, sociale et mentale.

Le piratage (hacking) et l'utilisation de faux profils Facebook ont été mis en avant comme facilitateurs d'intimidation, de harcèlement sexuel et d'extorsion. Les enfants ont fait preuve de responsabilité personnelle pour leur activité en ligne, mais ont reconnu que les enfants et les parents devraient être plus conscients des risques que pose Internet.

Il est important de noter que cette recherche révèle la nature sexospécifique de certains avantages et risques d'Internet. Par exemple, alors que les garçons sont les plus susceptibles de tirer des avantages commerciaux et financiers en ligne, les filles sont touchées de manière disproportionnée par le harcèlement sexuel et l'extorsion en ligne. En outre, le manque de sensibilisation aux garanties juridiques et aux mécanismes de signalement, associé aux normes sociétales patriarcales qui conduisent à blâmer les victimes, représente un obstacle important au signalement des cas d'extorsion en ligne.

Cette recherche a révélé un certain nombre de mécanismes existants et d'exemples positifs dans la prévention et la réponse à la violence en ligne en Tunisie. Il s'agit notamment des programmes existants de sensibilisation et de résilience prévus ou entrepris par le ministère de l'Éducation et le MFFES, notamment par l'intermédiaire du Centre national de l'informatique pour l'enfant (CNIPE), et grâce aux efforts de la société civile et au financement des ONG internationales. Cependant, ces campagnes sont souvent de courte durée et peu annoncées, ce qui entraîne leur manque de portée et d'impact. En outre, cette recherche a révélé un certain nombre d'initiatives prises par des acteurs individuels pour assurer la fourniture d'un soutien personnalisé aux enfants victimes et auteurs. Par exemple, certains juges des enfants et de la famille ont capitalisé sur leurs pouvoirs discrétionnaires pour fournir un soutien psychosocial ad hoc aux enfants qui ont été victimes de radicalisation en ligne ou qui se sont livrés à l'extorsion en ligne.

Malgré ces exemples positifs, cette recherche a révélé un certain nombre de lacunes juridiques et institutionnelles. Notamment, malgré la majorité des parties prenantes interrogées évaluant que le cadre juridique existant liés à la violence en ligne est adéquat, un consensus a émergé sur la nécessité de mettre à jour le code de la protection de l'enfance pour s'aligner sur l'avancement juridique. En outre, il exite un écart de mise en œuvre et de la nécessité de mettre à jour les mécanismes de réponse actuels pour s'aligner sur les avancées juridiques apportées par la loi organique n°58 -2017 du 22 août 2017 relative à l'élimination de la violence faite aux femmes, la loi organique n°61 de 2016 du 3 août 2016 sur la prévention et la lutte contre la traite des personnes et le décret-loi n° 2022-54 du 13 septembre 2022, relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication.

En outre, une lacune importante est apparue dans la fourniture des services aux victimes et notamment du soutien psychologique aux enfants. Les initiatives existantes, telles que les bureaux d'écoute et de conseil et les cellules d'écoute et de conseil, sont pratiquement abandonnées en raison du manque de personnel de soutien psychologique. Dans le même ordre d'idées, une prévention et

une réponse efficaces sont entravées par un manque de connaissances et de capacités techniques parmi les principales parties prenantes en matière de signalement et de traitement des matérielles d'exploitation sexuelle d'enfants en ligne. Ceci est particulièrement important car la recherche suggère des liens de causalité entre les enfants victimes de violence et les enfants qui deviennent auteurs de violence. De plus, les liens entre la violence en ligne et hors ligne, abordés plus en détail dans ce rapport et la revue de la littérature, nécessitent une réponse efficace à la violence en ligne.

4. Recommandations

Ce rapport propose un ensemble de recommandations, tirées des conclusions révélées dans cette recherche ainsi que des modèles internationaux et des exemples de meilleures pratiques. Compte tenu de l'importance et du manque de données systématiques et de recherches centrées sur les enfants sur les avantages et les risques associés à l'utilisation d'Internet, un investissement accru dans la recherche et la collecte de données est mis en évidence comme une condition préalable dans ce rapport. En outre, les recommandations avancées dans ce rapport sont divisées en 1) celles liées à la politique et à la législation, y compris la nécessité de réformer le Code de protection de l'enfance pour introduire la notion d'enfant victime, la nécessité de synchroniser les mécanismes de réponse existants pour s'aligner sur les avancées juridiques, et la nécessité de lignes directrices sur la protection de l'enfance en ligne pour l'industrie et les fournisseurs de services Internet, 2) celles liées au renforcement des capacités et au renforcement des systèmes, notamment par la formation des éducateurs et des juges, et l'amélioration de la littératie numérique chez les principaux acteurs gouvernementaux, 3) les recommandations de prévention et d'intervention, y compris la sensibilisation des enfants et des parents, l'amélioration de la résilience des enfants aux risques et aux préjudices en ligne et l'amélioration de la réponse psychosociale pour les enfants, et 4) des recommandations institutionnelles transversales soulignant la nécessité d'assurer une coordination intergouvernementale et d'intégrer la protection en ligne dans l'ensemble du système de protection de l'enfance.

I. Introduction

Ce rapport analyse les données qualitatives recueillies par Resolve Consulting et le Centre pour la justice et la prévention du crime (CJCP) dans le cadre du programme « Lutte contre la violence en ligne contre les enfants en Tunisie », mis en œuvre par le ministère de la Famille, de la Femme, de l'Enfance et des Seniors (MFFES) en partenariat avec l'UNICEF. Les conclusions et recommandations détaillées dans ce rapport constitueront la base d'un plan d'action national gouvernemental et multipartite pour prévenir et répondre à la violence en ligne contre les enfants en Tunisie.

1. Contexte de l'étude

Selon l'étude « la situation des enfants dans le monde » menée par l'UNICEF en 2017[1] , 1 internaute sur 3 est un enfant et chaque jour, plus de 175 000 enfants se connectent pour la première fois.[2] Les technologies de l'information et de la communication (TIC) sont au cœur de la vie quotidienne des enfants dans presque toutes les régions du monde. L'utilisation des TIC a transformé l'environnement dans lequel les enfants grandissent et se développent avec les technologies en ligne désormais intégrées dans les pratiques quotidiennes des jeunes dans leur communication, leur socialisation et leurs interactions avec le monde qui les entoure. Ce changement a été encore plus catalysé par la réponse de nombreux gouvernements, y compris le gouvernement tunisien, lors de la pandémie de COVID-19, où la communication, l'éducation et même le jeu des enfants se sont déplacés en ligne à un rythme sans précédent.

Même lorsque les enfants n'ont pas eux-mêmes accès à la technologie numérique, ils sont probablement touchés d'une manière ou d'une autre par l'utilisation de la technologie par d'autres membres de leur famille ou par le monde qui les entoure. Les enfants ont peu ou pas de choix quant à la façon dont la technologie fait partie de leur vie, et ils ne naissent pas non plus avec les compétences ou les connaissances inhérentes pour gérer les risques que présente la technologie.

Le monde dans lequel vivent les enfants n'est donc plus clairement délimité par ce qui se passe hors ligne et ce qui se passe en ligne. Pour comprendre la violence en ligne, telle que la cyberintimidation, l'exploitation sexuelle en ligne ou les abus sexuels basés sur l'image, en tant que nouvelles formes de violence qui se produisent en ligne, il est nécessaire d'examiner les moteurs et la relation entre les formes de violence qui se produisent en ligne et celles qui se produisent hors ligne.[3] La recherche sur la cyberintimidation, par exemple, a montré qu'il existe une forte relation entre les enfants qui intimident en ligne et ceux qui intimident hors ligne.[4] En outre, la sollicitation sexuelle des enfants, qui peut être initié en ligne, peut ensuite se déplacer hors ligne ou rester en ligne grâce à la diffusion en direct ou à d'autres formes d'abus.[5] L'intersection entre la violence en ligne et hors ligne est également reflétée par le nombre croissant de preuves sur la meilleure façon de prévenir et de répondre à la fois à la violence en ligne et hors ligne. Cela inclut la conceptualisation et la base de preuves sur ce qui fonctionne pour intervenir et prévenir la violence en ligne et hors ligne.

1 State of the World's Children 2017: Children in a Digital World. UNICEF, New York.https://www.unicef.org/sowc2017/
2 Safer Internet Day Press Release. UNICEF, New York, 6 February 2018. https://www.unicef.org/media/media_ 102560.html
3 Kardefelt-Winther, D., Maternowska, C. (2020) Addressing violence against children online and offline. Natural Human Behaviour 4, 227–230. https://doi.org/10.1038/s41562-019-0791-3 Haddon, L., and Livingstone, S. (2014) The relationship between
4 Haddon, L., and Livingstone, S. (2014) The relationship between offline and online risks. Young people, media and health: risks and rights: Nordicom Clearinghouse Yearbook 2014 (pp.21-32). Eds. C. von Feilitzen and J. Stenersen. Goteborg: Nordicom.
5 Kardefelt-Winther, D., Maternowska, C. (2020) Addressing violence against children online and offline. Natural Human Behaviour 4, 227–230. https://doi.org/10.1038/s41562-019-0791-3

À mesure que le discours sur les risques et les préjudices en ligne s'est développé, il existe un réel danger de marginaliser les droits et les opportunités d'accès et d'utilisation d'internet au nom de la sécurité. Les risques et les opportunités d'Internet ne sont ni binaires ni dichotomiques, et la compréhension des expériences en ligne des enfants, à la fois négatives et positives, est mieux comprise dans un cadre de droits et de protection de l'enfant.

> «Les droits de chaque enfant doivent être respectés, protégés et mis en œuvre dans l'environnement numérique. Les innovations dans le domaine des technologies numériques ont sur la vie et sur leurs droits des enfants d'importants effets, qui sont interdépendants, même lorsque les enfants n'accèdent pas eux-mêmes à l'Internet. Un accès effectif aux technologies numériques peut aider les enfants à réaliser l'ensemble de leurs droits civils, politiques, culturels, économiques et sociaux » (Article 4, Observation Générale n° 25 de 2021 sur les droits de l'enfant en relation avec l'environnement numérique)

L'Observation générale n° 25 s'appuie en outre sur l'article 12 de la Convention relative aux droits de l'enfant qui note que :

> «Les États parties devraient identifier les risques émergents auxquels les enfants font face dans divers contextes et y remédier, notamment en écoutant le point de vue des enfants sur la nature des risques particuliers auxquels ils font face » (Observation générale n° 25 III.C.14)

En outre, l'Observation générale n° 13 (2011) qui s'appuie sur l'article 19 de la Convention relative aux droits de l'enfant dispose ce qui suit :

> «Les États parties sont tenus, en vertu de la Convention, de combattre et d'éliminer la forte prévalence et l'incidence de la violence contre les enfants. L'application et la promotion des droits fondamentaux des enfants et le respect de leur dignité humaine et de leur intégrité physique et psychologique, par la prévention de toutes les formes de violence, sont essentiels à la promotion de l'ensemble des droits de l'enfant consacrés par la Convention » (Observation générale n° 13 III.13)

De plus, il est important de noter que les risques posés par la technologie aux enfants peuvent avoir un impact sur les enfants qui n'ont pas eux-mêmes accès à cette technologie. La sollicitation d'enfants à des fins d'exploitation sexuelle (grooming) peut se produire hors ligne, puis se déplacer vers l'espace virtuel. La cyberintimidation peut se produire par d'autres personnes utilisant des appareils mobiles ou d'autres formes de technologie tout en impliquant des victimes qui elles-mêmes n'ont pas un accès direct à cette technologie. En outre, bon nombre des compétences et des facteurs de protection dont les enfants ont besoin pour améliorer leur sécurité en ligne sont communs à ceux qui servent de facteurs de protection hors ligne, et les stratégies visant à assurer la sécurité des enfants doivent tenir compte de la manière dont leurs compétences et la résilience sont encouragées, hors ligne comme en ligne. Il est important que dans tous les aspects de toute politique ou stratégie visant à assurer la sécurité des enfants en ligne (et hors ligne), les besoins, les vulnérabilités et les facteurs de protection des enfants soient pris en compte dans leur intégralité.

Les enfants âgés de 5 à 17 ans constituent environ 20,3% de la population totale en Tunisie[6] En 2021, le pays avait un taux de pénétration total d'Internet de 66,7 %, et il est probable que cela se soit encore développé pendant la pandémie de COVID-19, car la vie quotidienne s'est déplacée en ligne à un rythme sans précédent. Selon une enquête de 2017[7] , les adolescents tunisiens âgés de 15 à 17 ans utilisent Internet 3 à 5 jours par semaine en moyenne, tandis que 43,9% utilisent quotidiennement les réseaux sociaux. De plus, le pourcentage de personnes (pas spécifiquement des enfants) qui ont utilisé Internet pour participer à des réseaux sociaux est passé de 66,6 % en 2019 à 78,4 % en 2020[8] .

Malgré l'augmentation documentée de la violence en ligne contre les enfants dans le monde, un rapport de l'UNICEF a souligné le manque de données systémiques spécifiques sur la violence en ligne affectant les enfants en Tunisie.[9] Les données existantes reflètent que les différentes formes de violence subies par les enfants en ligne sont de plus en plus préoccupantes et qu'un nombre croissant d'enfants en Tunisie risquent d'être victimes de violence en ligne. Par exemple, une enquête U-Report non représentative de 2020 auprès des enfants montre que 44 % des enfants interrogés ont déclaré avoir été victimes d'une forme de violence en ligne ou avoir été témoins de violence contre quelqu'un sur Internet, ces incidents se produisant principalement sur applications de médias sociaux. Bien que ces incidents puissent englober toute forme de violence en ligne, de la cyberintimidation ou du harcèlement à la violence sexuelle en ligne, un total de 164 562 signalements ont été faits à la ligne CyberTip basée aux États-Unis en relation avec du matériel d'abus sexuel d'enfants provenant de Tunisie ou impliquant des victimes ou des délinquants de La Tunisie en 2021.[10]

Cela met en évidence l'absence d'une stratégie et d'un mécanisme clairs pour identifier et documenter les différentes formes de violence et de menaces en ligne ciblant les enfants. Ceci, à son tour, entrave toute tentative de lutter efficacement contre ce phénomène d'une manière qui tienne compte simultanément du droit des enfants à accéder et à bénéficier d'Internet, et du droit à la protection contre les préjudices.

2. Objectifs de l'étude

Ce projet vise à soutenir le gouvernement tunisien, à travers la Politique Publique Intégrée de Prevention et de Protection de l'Enfance (PPIPPE)[11] et le programme pays 2021-2025 de l'UNICEF, dans le renforcement des capacités nationales de prévention, de détection et de réponse à la violence à l'égard des enfants, notamment par le biais d'une coordination multisectorielle et du changement des normes et comportements sociaux sur la violence contre les enfants.

En particulier, le projet vise à soutenir le MFFES pour renforcer la capacité des différents secteurs à faire face aux différents types de vulnérabilités et de violence contre les enfants dans le monde virtuel.

6 Kemp, Simon (2021) Numerqiue 2021: Tunisia. DataReportal. https://datareportal.com/reports/digital-2021-tunisia#:~:text=There%20were%207.92%20million%20internet,at%2066.7%25%20in%20January%202021.
7 UNICEF Tunisia (2020) Analysis of the situation of children in Tunisia. p. 128 https://www.unicef.org/tunisia/rapports/analyse-de-la-situation-des-enfants-en-tunisie-2020
8 Observatory of Information, Training, Documentation, and Studies for the Protection of the Rights of the Child (2022). p.17
9 UNICEF Tunisia (2020) Analysis of the situation of children in Tunisia. p. 128 https://www.unicef.org/tunisia/rapports/analyse-de-la-situation-des-enfants-en-tunisie-2020
10 National Center for Missing and Exploited Children. (2021) CyberTipline Reports by Country. Available at https://www.missingkids.org/content/dam/missingkids/pdfs/2021-reports-by-country.pdf
11 A l'heure d'écrire ce rapport la PPIPPE n'a pas encore été validée par le conseil ministériel

Ceci sera réalisé grâce à :

1. Une cartographie du contexte législatif et politique actuel, dans tous les secteurs concernés, pour prévenir et combattre la violence en ligne contre les enfants.[12]
2. Une évaluation des besoins actuels et des capacités des différents secteurs pour prévenir, répondre et soutenir les victimes de la violence en ligne contre les enfants.
3. Une exploration des expériences, des connaissances et des attitudes des enfants à l'égard de la violence en ligne et des comportements de recherche d'aide (recueillies lors de consultations avec des enfants).

Cela conduira à l'élaboration d'un plan d'action national (PAN) pour lutter contre la violence en ligne à l'égard des enfants en Tunisie.

L'étude répond à une série de questions :

- Dans quelle mesure la protection contre la violence en ligne (exploitation, violence et maltraitance des enfants en ligne) et la promotion de la sécurité en ligne sous toutes ses formes sont-elles intégrées dans la législation et la politique en Tunisie ?
- Dans quelle mesure les différents secteurs au sein du gouvernement, de la société civile et de l'industrie sont-ils conscients de leurs rôles et responsabilités, et capables de prévenir et de répondre à la violence en ligne contre les enfants ?
- Quelles mesures structurelles et organisationnelles et mécanismes de coordination existent pour assurer une réponse intersectorielle à la prévention de la violence en ligne contre les enfants en Tunisie (intergouvernementale et sociétale) ?
- En l'absence de données nationales ou infranationales, quelles sont les expériences en ligne, les connaissances et les capacités des enfants concernant leurs droits et leur protection en ligne, conformément à l'Observation générale n° 25 de la CRDE ?
- Quels sont les obstacles qui existent pour une réponse intersectorielle et pour prévenir et répondre à la violence en ligne contre les enfants en Tunisie, et comment peuvent-ils être surmontés compte tenu des contraintes existantes qui pourraient être rencontrées ?

3. Méthodologie de la recherche

L'examen de la littérature conceptuelle et des conventions internationales que la Tunisie a ratifiées (annexe 1), ainsi que la cartographie du cadre juridique et institutionnel tunisien de la protection de l'enfant et en ligne (annexe 2) ont facilité la conception d'une méthodologie de recherche adaptée à la collecte de données pour soutenir l'élaboration d'un plan d'action national.

La conception et la méthodologie de la recherche, y compris le protocole de recherche complet qui comprend tous les guides d'entretien et les questions du groupe de discussion, ont été partagées avec l'UNICEF Tunisie et le MFFES pour approbation.

12 Bien que cette note fasse référence à la violence en ligne contre les enfants, l'intersection entre la violence en ligne et hors ligne sera explicitement reconnue tout au long de ce travail.

En outre, l'équipe a soumis la méthodologie et le protocole de recherche pour une évaluation et un examen éthique par le HML Institutional Review Board (IRB).[13] Les protocoles de protection des sujets humains de cette étude ont reçu l'approbation de l'examen éthique du HML IRB le 26 juillet 2022 (numéro d'approbation #592TUNI22).

En raison 1) de l'intersection de la violence en ligne et hors ligne, et 2) des moteurs communs de la violence, de l'abus et de l'exploitation en ligne et hors ligne, cette recherche à viser à comprendre cette violence en gardant à l'esprit les perspectives de prévention et de réponse. Par conséquent, une analyse des facteurs de risque et de protection existants, dans les différents domaines dans lesquels les enfants vivent - individuel, familial et relationnel, communautaire et macro ou sociétal - doit être capturée. La méthodologie de recherche de Global Kids Online met l'accent sur la nécessité d'interroger les facteurs dans tous les secteurs susceptibles d'influencer la vie et le développement d'un enfant, de la santé à l'éducation en passant par la justice et les télécommunications. Par conséquent, il est nécessaire d'd'inclure les points de vue de personnes ayant une expertise et une expérience professionnelle dans ces domaines, en plus des décideurs politiques, des agents de protection de l'enfance et des prestataires de services. Les professionnels de la santé et de l'éducation constituent une interface importante avec les enfants, en particulier en ce qui concerne les comportements de recherche d'aide, et traitent directement les préjudices pouvant résulter d'expériences en ligne négatives. Les professionnels de la justice soulignent comment les lois sont mises en œuvre et si les décisions sont prises avec l'intérêt supérieur des enfants à cœur. Les représentants des télécoms expliquent comment ces entreprises fournissent un soutien ou sont des réponses aux problèmes de protection. En outre, saisir les points de vue des enfants sur la situation les défis et les expériences, ainsi que les mécanismes de prévention et de réponse existants évalue l'éventail des problèmes qui doivent être résolus et garantit que le plan d'action national inclut des perspectives centrées sur l'enfant. Cela a facilité une évaluation dans ce rapport des capacités existantes, des lacunes et de la direction qui peuvent être explorées en relation avec les cadres mondiaux pour la réponse au niveau des pays à la violence en ligne, y compris le modèle de réponse nationale (MRN) développé par l'Alliance mondiale WeProtect. Le MRN propose une approche intersectorielle pour prévenir et répondre à la violence en ligne contre les enfants et identifie les rôles des différents secteurs du gouvernement et de la société.

En plus de la revue de la littérature, l'équipe de recherche a recueilli des données qualitatives auprès des enfants, des parents, des enseignants et des principales parties prenantes impliquées dans tous les aspects de la protection en ligne des enfants. Cette collecte de données a consisté à :

- Entretiens avec les principales parties prenantes clés (EPPC) dans le domaine de la protection de l'enfance et des télécommunications
- Trois ensembles de groupes de discussion avec :
- Enfants (y compris une enquête anonyme à remplir par les participants)
- Enseignants et professionnels de l'éducation
- Parents

13 HML Institutional Review Board https://www.healthmedialabirb.com/

4. Entrevues avec les intervenants clés

L'entretien avec les parties prenantes clés (EPPC) est une méthode de recherche qualitative efficace et efficiente qui permet aux chercheurs d'obtenir des informations auprès des parties prenantes qui connaissent particulièrement le domaine et seront directement impactées par les recommandations politiques. Des EPPC approfondis ont été menés avec des experts et des informateurs qui possèdent des connaissances et des expériences pertinentes en matière de protection de l'enfance, d'éducation, de prévention et de réponse à la violence (en ligne). Les personnes interrogées comprenaient des parties prenantes clés au sein des divers ministères gouvernementaux, du système judiciaire, du système éducatif, des organismes de réglementation et des groupes de la société civile travaillant sur la protection de l'enfance et la prévention de la violence.

L'équipe de recherche a conçu un guide d'entretien semi-structuré (inclus dans le protocole de recherche en annexe 4) qui comprenait un ensemble de questions pour tous les entretiens et des questions spécifiques basées sur la profession de l'interviewé. Les entretiens ont exploré les perceptions des répondants sur l'ampleur et l'étendue du problème et les défis perçus pour lutter contre la violence en ligne. Celles-ci ont servi à explorer les perceptions et les connaissances des parties prenantes sur les risques et les préjudices subis par les enfants, ainsi que sur les rôles et responsabilités perçus. Les entretiens ont exploré plus en détail l'environnement politique et législatif et les lacunes de mise en œuvre, en s'appuyant sur la base de connaissances recueillie dans la revue de la littérature et la cartographie juridique et institutionnelle, et ont demandé quelle législation, selon eux, doit être introduite ou mieux mise en œuvre. En outre, la coordination et la collaboration entre les ministères, ainsi qu'entre le gouvernement, l'industrie et la société civile ont été explorées en détail. Après qu'une première liste de contacts ait été partagée par le MFFES le projet a suivi une approche d'échantillonnage en boule de neige. 17 entretiens et réunions formels ont été réalisés dans le cadre de cette recherche (annexe 5 pour une liste des personnes interrogées).

5. Groupes de discussion

Les groupes de discussion offrent une occasion importante de tester des compréhensions, des expériences et des messages particuliers concernant l'utilisation et la sécurité d'Internet. Cette méthode de recherche qualitative permet la collecte de données approfondies qui fournissent plus de détails sur le phénomène à l'étude que de larges questionnaires d'enquête.[14] De plus, les groupes de discussion sont la méthode la plus appropriée pour cette étude pour les raisons suivantes. Premièrement, comme il y a un manque de données centrées sur l'enfant en Tunisie sur l'expérience Internet des enfants, les groupes de discussion sont idéaux pour « une exploration en profondeur d'un sujet sur lequel on sait peu de choses. »[15] Ceci est particulièrement important car bien que la conception et les activités des groupes de discussion soient basées sur des études et des problèmes antérieurs que la recherche vise à explorer, « les groupes de discussion ont le potentiel de générer des résultats inattendus et imprévisibles à la fois en termes de données recueillies et de complexité du processus de recherche dans son ensemble. »[16]

14 Barbour, R. S. (1999). The use of focus groups to define patient needs. Journal of Paediatric Gastroenterology and Nutrition, 28, S19–22.
15 Stewart and Shamdasani (1990) p. 102.
16 Parker and Tritter (2006) p.34.

Cela garantit que la recherche teste de manière déductive les hypothèses de recherche et permet aux participants d'influencer de manière inductive la trajectoire de la recherche et, en fin de compte, du plan d'action national.

Deuxièmement, les groupes de discussion sont une méthode éthiquement responsable pour mener des recherches avec des mineurs. En effet, les GD peuvent aider à « créer un environnement de pairs sûr pour les enfants »[17] et à corriger les « déséquilibres de pouvoir entre les chercheurs et les participants»[18] qui existeraient dans un entretien individuel entre un adulte et un enfant. Troisièmement, c'est une méthode inclusive parce qu'elle est adaptée aux personnes handicapées, telles que les déficiences visuelles ou de communication ou les personnes ayant des problèmes d'écriture ou de lecture,[19] et les personnes vulnérables. Quatrièmement, des études qualitatives similaires sur l'expérience en ligne des enfants dans d'autres pays utilisent des groupes de discussion, souvent en plus des entretiens individuels. Stoilova et al (2019) ont utilisé des « groupes de discussion parce qu'il y a un manque de compréhension suffisante de la relation entre l'utilisation de la technologie numérique et les problèmes de santé mentale à l'adolescence » [20] et Global Kids Online (2016) a conçu un cadre qui comprenait des groupes de discussion pour permettre une flexibilité en cherchant à « comprendre [...] les droits des enfants à l'ère numérique. »[21]

L'étude de Livingstone sur les données et la vie privée des enfants en ligne a organisé des groupes de discussion avec des enfants, des parents et des éducateurs pour soutenir l'élaboration de « politiques inclusives pour les enfants et de recommandations éducatives/de sensibilisation »[22] .

Les sites de recherche ont été déterminés après de longues consultations et discussions avec le MFFES. Les lieux des groupes de discussion de Gafsa, Kasserine, Jendouba et du Grand Tunis ont été sélectionnés sur la base de trois indicateurs importants et interconnectés relatifs à la vulnérabilité des enfants établis en consultation avec le MFFES [23] : les indicateurs de développement régional, le taux de réussite au baccalauréat et le taux d'abandon scolaire. [24] Cela a permis aux groupes de discussion de répondre aux besoins de recherche tout en tenant compte des limites budgétaires et temporelles. Les trois indicateurs pour la sélection des sites de recherche sont discutés en détail dans l'annexe 3.

5.1. Groupes de discussion avec des enfants

L'équipe de recherche a organisé 16 groupes de discussion avec 113 enfants âgés de 13 à 17 ans, dont 64 filles et 49 garçons dans quatre sites de recherche dans cinq gouvernorats : Grand Tunis (Tunis, Manouba), Kasserine, Gafsa et Jendouba. Les groupes de discussion avec des enfants visaient à comprendre comment les enfants en Tunisie utilisent Internet, à quelles fins, s'ils prennent des risques et s'ils ont été exposés à des préjudices.

17 Adler, K., Salanterä, S., & Zumstein-Shaha, M. (2019). Focus Group Interviews in Child, Youth, and Parent Research: An Integrative Literature Review. International Journal of Qualitative Methods, 18. p.2.
18 Shaw, C., Brady, L.-M., & Davey, C. (2011). Guidelines for research with children and young people. NCB Research Centre. London, England: National Children's Bureau. p.4.
19 Adler, K., Salanterä, S., & Zumstein-Shaha, M. (2019). p.1.
20 Stoilova, M., Edwards, C., Kostyrka-Allchorne, K., Livingstone, S., & Sonuga-Barke, E. (2021) Adolescents' mental health vulnerabilities and the experience and impact of digital technologies: A multimethod pilot study. London School of Economics and Political Science and King's College London. p.79.
21 Stoilova, M., Livingstone, S., & Kardefelt-Winther, D. (2016). Global Kids Online: Researching children's rights globally in the digital age. Global Studies of Childhood, 6(4), p.460.
22 Livingstone, S. Stoilova, M. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age. An evidence review. London: London School of Economics and Political Science.
23 Réunion de projet 29 août 2022
24 La pertinence et l'application de ces indicateurs à la sélection des sites sont explorées plus en détail à l'annexe 1.

L'échantillon de chaque site a assuré une répartition équitable selon le sexe et l'âge. Dans chacun des sites sélectionnés, l'équipe a mené trois groupes de discussion : garçons uniquement, filles uniquement et un groupe mixte garçon/fille. Alors que les modérateurs des GD se sont efforcés de créer un espace sûr pour toutes les discussions, l'inclusion d'un groupe réservé aux filles a assuré un espace sûr et confortable pour discuter ouvertement de leurs expériences et de leurs connaissances. Ceci est important car des différences entre les sexes peuvent survenir dans des groupes d'adolescents ou lors de discussions sur des sujets spécifiques au sexe.[25] Par conséquent, nous avons émis l'hypothèse que les différentes compositions par sexe des groupes produiraient des résultats différents, conduisant ainsi à un ensemble de données plus complet et plus riche. Le sexe du modérateur du groupe de discussion peut également influencer la collecte de données. [26]Ainsi, alors qu'un modérateur animait certains des groupes mixtes, tous les groupes de filles étaient animés par une modératrice.

L'équipe a travaillé avec des organisations et institutions partenaires, telles que des collèges et le Centre National de l'informatique pour l'Enfant (CNIPE) et ses centres régionaux (CRIPE), pour coordonner et organiser les groupes de discussion. De plus, pour assurer la diversification des enfants répondants et l'inclusion des enfants vulnérables, l'équipe de recherche s'est coordonnée avec le Centre Intégré de la Jeunesse et de l'Enfance Cité el Khadra pour organiser trois groupes de discussion.

Les discussions du groupe de discussion se sont déroulées en arabe tunisien, la langue que les enfants parlaient avec le plus d'aise. Avec la permission des participants, les discussions du GD ont été enregistrées en audio. Les groupes de discussion comprenaient entre quatre et 13 participants chacun.

Au début de chaque GD, les enfants ont reçu une courte enquête sur leurs habitudes et leur fréquence d'utilisation d'Internet. Cela visait à permettre aux participants de réfléchir à leur utilisation d'Internet. Le protocole de recherche a été testé sur un groupe de discussion pilote de six participants. Cela a conduit l'équipe de recherche à introduire plusieurs modifications à la méthodologie de recherche initiale, principalement en réduisant la longueur et en évitant les répétitions. Les groupes de discussion avec les enfants étaient basés sur quatre grands points de discussion/activités :

- Introduction : y compris les applications/plateformes de médias sociaux qu'ils utilisent le plus et quelles sont leurs principales raisons d'utiliser Internet ;
- Bénéfices et risques : sur des post-it, les participants écrivent respectivement les bénéfices et les risques (un par post-it) liés à l'utilisation d'internet/des réseaux sociaux. À l'aide d'un tableau à feuilles mobiles, avec une ligne horizontale divisant le papier en deux avec un visage heureux dessiné à gauche et un visage triste à droite, les participants placent leurs post-it du côté approprié. Les avantages ont d'abord été longuement discutés avant de passer aux risques;
- Protection des données : les participants discutent de ce qu'Internet sait d'eux et des mesures qu'ils prennent pour protéger leurs données personnelles et leur sécurité ;
- Un meilleur Internet : les participants ont été invités à discuter des améliorations qu'ils souhaitent voir apportées à Internet pour améliorer leur sécurité.

25 Fielden, A. L., Sillence, E., & Little, L. (2011). Children's understandings' of obesity, a thematic analysis. International Journal of Qualitative Studies on Health and Well-Being, 6.
26 Adler, K., Salanterä, S., & Zumstein-Shaha, M. (2019). Focus Group Interviews in Child, Youth, and Parent Research: An Integrative Literature Review. International Journal of Qualitative Methods, 18. p.4.

À la fin de chaque GD, les enfants ont rempli un questionnaire d'auto-évaluation anonyme de 19 items pour répondre à des questions plus sensibles sur les expériences négatives des enfants en ligne. Cela comprenait une question ouverte sur les expériences qu'ils pourraient ne pas se sentir à l'aise de révéler devant leurs pairs.

5.2. Groupes de discussion avec les parents

L'équipe de recherche a organisé quatre GD avec 28 parents (sept pères, 21 mères). Les GD avec les parents visaient à explorer ce qui préoccupe les parents en ce qui concerne l'utilisation et les expériences des médias sociaux des enfants, et comment cela s'aligne sur les expériences des enfants. Ces groupes de discussion ont cherché à explorer la compréhension et les connaissances des parents sur l'utilisation des médias sociaux et de la technologie numérique par leurs enfants, en plus des stratégies qu'ils emploient pour gérer les risques associés tout en maximisant les avantages.

Les GD avec les parents étaient basés sur trois points de discussion/activités :

- Introduction : comment ils utilisent les médias sociaux et ce qu'ils apprécient le plus dans les médias sociaux.
- Gérer l'utilisation d'Internet des enfants : explorer la compréhension et les connaissances des parents sur les médias sociaux et la technologie numérique de leurs enfants et les stratégies de gestion qu'ils emploient. Cette discussion visait à explorer les points de vue des parents sur les opportunités et les avantages que les médias sociaux offrent à leurs enfants, ainsi que les connaissances et les attitudes des parents à l'égard de l'utilisation des médias sociaux par leurs enfants. Elle visait également à discuter de toute expérience négative que leurs enfants auraient pu rencontrer et à explorer les stratégies que les parents adoptent pour atténuer ces risques en ligne et s'assurer que leurs enfants peuvent utiliser les réseaux sociaux en toute sécurité.
- Résumé de la discussion : clarifier les principaux points discutés lors du focus group et souligner les aspects positifs partagés.

5.3. Groupes de discussion avec des éducateurs

L'équipe de recherche a organisé trois GD avec 22 éducateurs (huit hommes, 14 femmes). Les groupes de discussion avec les enseignants visaient à parler aux personnes qui éduquent ou soutiennent les enfants, telles que les enseignants, les conseillers scolaires et les travailleurs sociaux, sur leurs perceptions et leurs expériences des activités et des expériences des enfants sur les réseaux sociaux. Les GD avec les éducateurs suivaient une structure similaire à celle des GD avec les parents.

5.4. Éthique et protection de l'enfance

Comme mentionné ci-dessus, les protocoles de protection des sujets humains dans cette recherche ont été évalués dans le cadre d'un examen éthique de la recherche par le HML Institutional Review Board (IRB) et ont reçu l'approbation éthique le 26 juillet 2022 (numéro d'approbation #592TUNI22).

En plus de veiller à ce que la conception de la recherche soit alignée sur les directives éthiques de la recherche pour la protection des sujets humains, une attention particulière a été accordée par l'équipe de recherche à la sécurité et à la confidentialité des groupes de discussion d'enfants. En raison de la sensibilité potentielle du sujet, la confidentialité des répondants est essentielle. Par conséquent, au début de chaque GD d'enfants, les participants ont été invités à choisir un pseudonyme/faux nom à utiliser dans la rédaction du rapport. Par conséquent, les noms des enfants apparaissant dans ce rapport sont tous des pseudonymes choisis par les enfants eux-mêmes. À la fin de l'auto-questionnaire, l'aide confidentielle suivante a été offerte aux jeunes participants.

> « Est-ce que quelque chose dont vous avez parlé aujourd'hui vous dérange ? N'oubliez pas que vous pouvez parler au facilitateur une fois que vous avez terminé ici, et il ou elle peut vous aider à trouver quelqu'un à qui parler en privé et de manière anonyme ! »

Deux enfants participant à un groupe de discussion réservé aux femmes ont demandé un soutien psychologique confidentiel. L'équipe de recherche a coordonnée avec l'UNICEF et le MFFES et a identifié un psychologue affilié au ministère dans leur région. Nous continuons à nous coordonner avec les deux enfants pour nous assurer qu'elles reçoivent le suivi psychologique nécessaire.

6. L'analyse des données

Les données des groupes de discussion et des entretiens ont fait l'objet d'une analyse déductive et inductive à l'aide du logiciel d'analyse qualitative NVIVO 12. Au premier niveau d'analyse, l'équipe de recherche a codé les données dans des codes déductifs prédéterminés : avantages de l'utilisation d'Internet, risques et inconvénients associés à l'utilisation d'Internet, les mesures et politiques existantes, les lacunes existantes et les recommandations. Les constatations sous chacun des codes des avantages et des risques sont élaborées en détail dans chaque sous-section de la section résultats de la recherche du présent rapport. Les résultats sous les codes des mesures et politiques existantes, ainsi que les lacunes existantes, sont discutés dans la section 3. Dans une deuxième étape de l'analyse, les données sous chaque code ont été analysées plus en détail et l'équipe de recherche a extrait des sous-codes inductifs pour chaque code. Dans certains cas, les sous-codes ont été divisés en d'autres sous-codes.

De plus, les données de la pré-enquête du groupe de discussion sur les enfants et du questionnaire anonyme ont été entrées dans Excel et les tendances ont été révélées grâce à l'utilisation d'outils d'analyse quantitative avancés d'Excel.

7. Limites de la méthodologie

Cette recherche adopte une méthodologie qualitative qui vise à produire des données approfondies et centrées sur l'enfant, y compris une description détaillée des récits et expériences personnels. La recherche ne prétend pas être représentative de l'enfance tunisienne, mais la sélection de cas des gouvernorats, basée sur l'intersection de trois indicateurs pertinents liés à la violence des enfants, et l'éventail des jeunes participants, garantit que les données collectées sont à la fois spécifiques aux cas individuels et indicatif d'un contexte national plus large.

En ce qui concerne les données d'enquête collectées à partir du questionnaire anonyme, la petite taille de l'échantillon par rapport à la population nationale rend ces données non représentatives. Cependant, le questionnaire a permis aux enfants, par le biais d'une question ouverte, de partager en toute sécurité et de manière anonyme des expériences sensibles ou bouleversantes qu'ils n'auraient peut-être pas senti à l'aise de partager dans le cadre du GD Toutes les réponses qualitatives sont listées en annexe 6. En outre, l'enquête fournit une indication de l'exposition ou de la génération de contenu, de textes ou d'autres éléments perturbateurs à caractère sexuel qui n'ont peut-être pas été abordés dans les discussions des GD. Il convient toutefois de noter que la Tunisie fait partie des pays inclus dans l'étude quantitative intitulée «Disrupting Harm» prévue pour 2023-2024 qui produira des données représentatives sur la violence en ligne contre les enfants.

II. Avantages et risques d'Internet : une perspective centrée sur l'enfant

Afin de faire progresser une compréhension centrée sur les enfants des expériences positives et négatives des enfants en ligne, l'analyse et le codage des données des groupes de discussion avec des enfants se sont concentrés sur la révélation des perspectives et des expériences des enfants concernant les avantages, les risques et les méfaits associés à l'utilisation d'Internet. Celles-ci sont respectivement décrites dans les deux sous-sections suivantes. Le cas échéant, l'analyse des données des groupes de discussion d'enfants est juxtaposée aux conclusions des groupes de discussion de parents et d'éducateurs, soulignant les lacunes qui existent dans la compréhension des expériences des enfants avec Internet et son impact.

1. Avec modération, l'utilisation d'Internet offre de nombreux avantages éducatifs, sociaux et économiques

Les discussions de groupe avec les enseignants et les parents ont révélé une réticence initiale de leur part à reconnaître et à discuter des impacts positifs de l'utilisation d'Internet sur la vie des enfants. Lorsque le facilitateur a incité et sondé à tenir une discussion sur les avantages perçus, les discussions ont souvent été largement limitées aux avantages éducatifs et à la facilité d'accès à l'information. Ceux-ci ont été discutés en termes généraux, révélant un manque général d'engagement des parents et du personnel éducatif avec les outils et sources en ligne spécifiques utilisés par les enfants pour améliorer leur expérience éducative et accéder aux informations.

Les groupes de discussion des enfants ont corroboré les perceptions des parents et des enseignants sur les avantages éducatifs d'Internet. Cependant, les discussions avec les enfants ont produit des données et des conclusions beaucoup plus riches sur les outils et mesures spécifiques qu'ils utilisent pour faire progresser et compléter leur apprentissage scolaire via Internet. En outre, l'analyse des groupes de discussion d'enfants a révélé un éventail d'autres avantages dans tous les domaines de leur vie, qui n'ont pas été mentionnés ou ne sont pas connus de leurs parents et éducateurs.

2. Avantages éducatifs

2.1. Améliorer l'apprentissage lié à l'école

Les enfants ont signalé plusieurs avantages éducatifs de l'utilisation d'Internet, la majorité utilisant Google et des sites web éducatifs (tels que TakiAcademy) pour effectuer des recherches et améliorer leur compréhension de leurs leçons ou comprendre leurs devoirs. YouTube a également été noté comme un sitewWeb important pour l'apprentissage ou l'aide aux devoirs dans les groupes de discussion. En particulier, GD 8 a mentionné les chaînes YouTube dédiées à l'explication du matériel scolaire.

Il convient de noter que cet avantage a été mis en garde dans certains GD et que des discussions ont suivi sur les limites de l'utilisation d'Internet pour améliorer l'apprentissage scolaire. Par exemple, dans GD7, les participants ont convenu que, même si l'utilisation d'Internet pour faire leurs devoirs peut être utile, certains étudiants peuvent abuser de cet outil, copiant aveuglément des leçons entières et des travaux de recherche sans absorber les informations. Cela a été mis en évidence dans une interview avec Mme Najet Souli, professeure émérite principale, qui s'est plainte que «de nos jours, si un enfant a pour devoir de faire des recherches sur une plante ou sur les différentes espèces d'animaux herbivores et carnivores, il ira au cybercafé et pour récupérer un document de recherche complet pour 2 TND. 90% des informations ne colleront pas » (entretien avec un chercheur).

Amélioration des compétences linguistiques

La majorité des enfants ont signalé des avantages liés à l'apprentissage des langues via des applications de traduction, des outils d'apprentissage des langues comme Simply, Duolingo, Google Translate et Memrize, en regardant du contenu en langue étrangère ou en communiquant sur les réseaux sociaux et via les jeux en ligne. Comme l'a indiqué Jako, «mon anglais s'est vraiment amélioré car je me fais toujours de nouveaux amis et je discute avec eux tout en jouant à des jeux vidéo» (17 ans, garçon).

Amélioration des connaissances générales et des compétences

De nombreux enfants ont déclaré utiliser Internet pour se tenir au courant de l'actualité, suivre les sujets qui les intéressaient et acquérir de nouvelles compétences tout en perfectionnant celles qui existent déjà (peinture, cuisine, échecs, photographie, production et montage vidéo, design, danse et maquillage). Comme l'a expliqué Donya, «je m'intéresse à l'actualité et je suis intéressé par ce qui se passe dans le pays et dans le monde. Les réseaux sociaux m'aident à rester informé» (16 ans, fille). De même, Duma a indiqué que «j'adore cuisiner et j'ai appris tellement de recettes différentes en ligne» (14 ans, garçon).

Améliorer la compréhension et l'ouverture aux différentes cultures

Que ce soit en se faisant des amis en ligne de différents pays et milieux culturels ou en regardant des séries et des films, la majorité des enfants ont signalé une meilleure compréhension des différentes cultures et une appréciation de la diversité. Cet avantage a été particulièrement mis en évidence parmi les participants des zones rurales et des régions de l'intérieur, sans doute en raison de leur marginalisation socio-économique qui limite leurs déplacements et leurs possibilités de rencontrer diverses personnes directement. En effet, comme l'a déclaré un participant de la région rurale de Manouba à Tebourba, «Internet me fait découvrir de nouvelles choses que je n'aurais jamais rencontrées dans la vraie vie autrement» (Zarga, 17 ans, garçon). Les participants au GD6 ont également déclaré avoir élargi leurs horizons en nouant de nouvelles amitiés à travers le monde. Cela reflète les découvertes d'autres pays, où les enfants considèrent Internet comme le seul moyen d'élargir leur monde, et où rencontrer de nouveaux amis en ligne, d'autres cultures et régions, est l'un des principaux atouts d'être en ligne [27].

> L'UN DES AVANTAGES D'ETRE EN LIGNE, POUR DE NOMBREUX ENFANTS EN TUNISIE ETAIT DE RENCONTRER D'AUTRES PERSONNES DE DIFFERENTES REGIONS DU MONDE ET D'AUTRES CULTURES. CECI EST PARTICULIEREMENT IMPORTANT POUR CEUX QUI VIVENT DANS DES COMMUNAUTES RURALES OU MARGINALISEES. POURTANT, CELA REFLETE EGALEMENT L'UNE DES TENSIONS APPARENTES DANS LES APPROCHES COURANTES DE LA SECURITE SUR INTERNET.
>
> L'UN DES PRINCIPAUX MESSAGES DE NOMBREUSES CAMPAGNES DE SECURITE EN LIGNE, ET L'UN DES PRIORITES DE NOMBREUX PARENTS ET ENSEIGNANTS, EST L'IDEE DE « DANGER ETRANGER », ET LES ENFANTS SONT DECOURAGES DE PARLER A DES ETRANGERS EN LIGNE. POURTANT, LA MAJORITE DES RISQUES SEXUELS AUXQUELS LES ENFANTS SONT CONFRONTES VIENNENT DE PERSONNES QU'ILS CONNAISSENT, PLUTOT QUE D'ETRANGERS (OMS, 2022). CE N'EST QU'UN EXEMPLE DE LA FAÇON DONT LA SENSIBILISATION QUI N'A AUCUN FONDEMENT DANS LA PREUVE, PEUT INHIBER L'UN DES PRINCIPAUX AVANTAGES POUR LES ENFANTS, PLUTOT QUE DE LES DOTER DES COMPETENCES NECESSAIRES POUR GERER LES INTERACTIONS QU'ILS ONT EN LIGNE, DE MANIERE SURE ET INFORMEE.

27 Burton, P., Leoschut, L. & Phyfer, J. (2016). South African Kids Online: A glimpse into children's internet use and online activities. Cape Town: The Centre for Justice and Crime Prevention.

2.2. Bénéfices sociaux : Entretenir et construire des relations sociales

La plupart des participants utilisent les médias sociaux principalement pour rester en contact avec leurs amis et leur famille, la majorité déclarant établir activement ou organiquement de nouvelles relations et développer des amitiés en ligne. Par exemple, Arij a déclaré que «ma tante vit à l'étranger et pendant les célébrations religieuses comme l'Aid, elle nous manque et nous lui manquons, alors nous l'appelons sur Facebook et elle peut passer du temps avec nous à l'autre bout du fil, comme si elle est avec nous» (17 ans, fille). Cela procure des avantages sociaux et émotionnels en permettant aux enfants de se sentir connectés et de développer un sentiment d'appartenance. Cela est conforme aux conclusions de l'étude Global Kids Online menée dans 11 pays, qui montre que les réseaux sociaux et les plateformes de chat sont devenus un lieu de rencontre crucial où les enfants peuvent se rencontrer et socialiser avec leurs amis et leur famille[28] .

3. Divertissement

Les participants ont énuméré les nombreuses façons dont Internet offre une source de divertissement. Cela comprenait des activités passives telles qu'écouter de la musique, regarder des vidéos, regarder des séries et des films et regarder du sport. En outre, des formes interactives de divertissement telles que faire des entraînements / exercices, apprendre des routines de danse, jouer et chercher de l'inspiration pour l'art et la mode ont été citées. Regarder du contenu (des memes et des vidéos) par des « influenceurs » sociaux, en plus de créer, éditer et publier leur propre contenu sur les réseaux sociaux, ont également été fréquemment mentionnés. Le fait que ces enfants s'engagent activement dans la création, l'édition et l'interaction avec des memes et d'autres contenus indique qu'il existe un certain niveau de compétences techniques créatives appliquées de manière régulière, reflétant ainsi à la fois l'opportunité de divertissement et l'expression d'un certain niveau de créativité, ainsi que des compétences au-delà de la simple consommation de médias.

Les participants au GD 10 ont convenu qu'Internet les protégeait chez eux et les éloignait de tous les problèmes qu'ils pouvaient rencontrer à l'extérieur. Comme l'a dit un participant, « il n'y a rien de bon à l'extérieur à Kasserine, que des problèmes » (John, 17 ans, garçon). Les participants ont expliqué qu'ils n'avaient aucun moyen de se divertir et qu'« avant, nous allions au moins gratuitement à la Maison de Jeunes. Maintenant, si tu veux aller à la Maison des Jeunes, tu dois payer 5 dinars par jour » (John, 17 ans). De plus, comme l'explique Kortli, « chaque quartier de Kasserine est contrôlé par un groupe de garçons, qui vous tabasseront si vous venez sur leur territoire » (17, garçon, GD 10). Internet offre à ces enfants un moyen pratique d'échapper aux sévices physiques et de jouer dans un espace sûr.

3.1. Avantages commerciaux et gain monétaire

Un certain nombre de participants ont rapporté comment Internet les avait aidés à développer leurs compétences professionnelles et entrepreneuriales. Cela a par la suite facilité leurs activités, leur permettant de recevoir des avantages financiers directs ou indirects de leur utilisation d'Internet. Certains participants ont appris et développé des compétences (photographie, codage

28 Kardefelt Winther, Daniel; Livingstone, Sonia; Saeed, Marium (2019). Growing up in a connected world, Innocenti Research Report, UNICEF Office of Research - Innocenti, Florence. Pg. 16. https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf

et développement d'applications) en ligne et ont lancé des carrières indépendantes en monétisant leurs compétences. En tant que peintre en bâtiment, et bien que son travail à temps partiel ne nécessite pas Internet, Pastis (17 ans, garçon), a déclaré que son entreprise bénéficiait et attirait de nouveaux clients grâce à la visibilité que lui procuraient les médias sociaux. D'autres participants gagnaient de l'argent grâce au jeu, comme Jako (17 ans, garçon) qui collectionne et vend des diamants sur le jeu populaire Free Fire. Recevoir de l'argent publicitaire grâce à la réalisation de vidéos et augmenter l'exposition pour attirer plus de clients ont également été mentionnés comme des avantages financiers.

Notamment, l'entrepreneuriat en ligne était largement limité aux participants masculins. La plupart des participantes qui utilisent les médias sociaux pour publier des informations sur leurs produits (tels que des peintures, des photographies, des bijoux faits à la main) le font sans intention de vendre ou de réaliser un gain financier. Cependant, les participantes au GD 8 (filles uniquement) ont convenu qu'Internet facilite l'achat et la vente d'articles. Cela reflète un clivage potentiel entre les sexes dans la manière dont les enfants utilisent les opportunités commerciales potentielles qu'offre Internet aux enfants. Une meilleure compréhension de cette dynamique émergente serait nécessaire afin de s'assurer que les garçons et les filles sont en mesure de tirer le meilleur parti de cet aspect de l'internet et de la connectivité numérique.

3.2. Avantages pour la santé mentale

Les participants ont mentionné les diverses façons dont Internet offre des moyens d'améliorer leur santé mentale. Les participants au GD 5 ont expliqué comment regarder des vidéos divertissantes les aide à se détendre. Les participants du centre intégré (GD 2) ont cité le fait de passer le temps le « retrait de la réalité » comme des avantages des médias sociaux, suggérant peut-être la difficile réalité sociale de ces enfants institutionnalisés et leur réconfort dans les médias sociaux. Les participants au GD 4 ont également mentionné comment Internet leur a permis « d'échapper à la réalité. »

Plusieurs groupes de discussion ont discuté des avantages des divers groupes de soutien en ligne, permettant aux gens de s'entraider et de s'offrir des conseils. Ces groupes mettent en relation les personnes qui ont besoin d'aide avec d'autres désireuses et capables de fournir cette aide. Les participants au GD 5 ont mentionné que le fait de recevoir des «j'aime» sur des photos d'eux-mêmes augmentait leur estime de soi et qu'ils trouvaient certains avantages pour la santé mentale à publier sur les moments difficiles qu'ils traversaient. GD 6 a rapporté que rester en contact avec des amis et nouer de nouvelles amitiés améliorait leur estime de soi et leur sentiment d'appartenance.

La complexité de la technologie numérique, de l'utilisation d'Internet et de la santé mentale est souvent simplifiée à l'extrême, réduite aux conséquences plus négatives d'une utilisation excessive d'Internet et de l'exposition à un contenu « déclencheur », souvent organisé de manière algorithmique.[29] Pourtant, comme en témoigne cette recherche, Internet peut souvent être un refuge ou offrir un espace sûr, où les enfants peuvent trouver du soutien et échapper à des situations difficiles hors ligne.

29 Vuorre, M., Orben, A., & Przybylski, A. K. (2021). There Is No Evidence That Associations Between Adolescents' Digital Technology Engagement and Mental Health Problems Have Increased. Clinical Psychological Science, 9(5), 823–835. https://doi.org/10.1177/2167702621994549

La mesure dans laquelle les enfants peuvent maximiser les avantages, en particulier ceux qui éprouvent des difficultés de santé mentale, peut souvent dépendre de leurs compétences numériques et de la manière dont ils les appliquent. Il devient donc encore plus important d'aider les enfants à développer ces compétences.[30]

4. L'utilisation d'Internet est associée à des risques et des préjudices physiques, mentaux et psychologiques nouveaux et accrus

Bien que les avantages d'une utilisation modérée d'Internet soient abondants, les groupes de discussion et les entretiens ont révélé des dommages et des risques importants en ligne. L'analyse thématique des données des groupes de discussion a produit les sous-codes de « risques et préjudices » suivants.

4.1. Utilisation excessive

La majorité des participants ont souligné les effets néfastes d'une utilisation prolongée d'Internet sur leur santé physique. Ceux-ci incluent des problèmes de vue, des maux de dos et une mauvaise posture, des problèmes de colonne vertébrale, une prise de poids et des maux de tête, en plus des problèmes de concentration et de la perte de mémoire.

De plus, la « dépendance » (le terme 'iidman utilisé par les participants) a été citée comme un risque clé dans les groupes de discussion d'enfants, d'enseignants et de parents. Les participants ont défini la dépendance à Internet comme une utilisation excessive et/ou une dépendance à Internet entraînant des effets négatifs sur les relations sociales, les fonctions cognitives, le niveau d'instruction et la santé physique. Il y avait un accord général sur le fait que, si l'utilisation d'Internet avec modération débloque un éventail d'avantages pour les utilisateurs, la dépendance à Internet peut isoler les utilisateurs de leur famille et de leurs amis. Alors que la majorité des participants conviennent que les médias sociaux leur permettent de rester en contact avec leurs amis et leur famille, ils ont également cité le rôle des médias sociaux et d'Internet dans l'isolement et l'érosion des liens en personne entre amis et famille. L'impact sur certaines familles et certains enfants peut être dévastateur. Comme l'a expliqué une participante d'un centre pour enfants sans soutien familial, « ma mère a commencé à utiliser cette application grâce à laquelle elle a rencontré et discuté avec des gens du monde entier. Elle en est devenue tellement dépendante qu'elle s'est retirée de moi et de mes frères et sœurs jusqu'à ce que cela est devenu de la négligence envers les enfants, et nous lui avons été enlevés » (Yasmine, 14 ans, femme).

> Ma mère a commencé à utiliser cette application où elle a rencontré et discuté avec des gens du monde entier. Elle en est devenue dépendante et s'est retirée de moi et de mes frères et sœurs jusqu'à ce que cela est devenu de la négligence envers les enfants, et nous lui avons été enlevés » (Yasmin, 14 ans).

30 Livingstone, S., Stoilova, M., Stänicke, L. I., Jessen, R. S., Graham, R., Staksrud, E., & Jensen, T. K. (2022). Young people experiencing internet-related mental health difficulties: The benefits and risks of digital skills. An empirical study. KU Leuven, ySKILLS.

Les participants pensaient également que la consommation excessive et la dépendance peuvent distraire les enfants de leurs études tout en retardant la croissance mentale et sociale et les soins personnels. De plus, les participants ont établi un lien entre l'utilisation excessive d'Internet et une mauvaise concentration et des problèmes psychologiques.

Alors que les participants au GD 4 ont cité l'Internet leur permettant d' « échapper à la réalité » comme un avantage, ils ont également indiqué qu'une utilisation excessive peut devenir malsain, affirmant que certaines personnes subissent même des changements de personnalité en raison de leur isolement et de leur dépendance à Internet. Les participants ont noté qu'Internet peut faciliter l'utilisation excessive ou la dépendance aux jeux, à regarder des émissions ou à du matériel pornographique. Ils ont également noté que cela posait des risques financiers, tels que dépenser trop d'argent pour les jeux en ligne.

Cette recherche a aussi mis en évidence une idée fausse largement répandue en Tunisie selon laquelle une utilisation excessive d'Internet cause l'autisme. Dans tous les GD d'enfants et de parents qui ont discuté de l'autisme, les participants ont lié à tort la dépendance à Internet à l'apparition des troubles du spectre autistique (TSA). Le TSA est un trouble biologique du développement cérébral qui est très probablement causé par une combinaison de facteurs génétiques et environnementaux de l'enfant pendant la grossesse. [31] Cela signifie qu'il ne peut être causé, par aucun facteur, chez les enfants. L'origine de la perception générale - qu'un excès d'Internet, ou de temps passé devant un écran, cause l'autisme - peut être due au fait que les personnes autistes ont tendance à utiliser davantage Internet car elles trouvent les interactions de personne à personne plus difficiles.[32][33] Par exemple, « les adolescents autistes passent plus de temps à jouer en ligne que leurs pairs neurotypiques. [34]» De plus, le temps passé devant un écran agit comme un stimulant et, en excès, peut exacerber les symptômes puisque les enfants atteints de TSA sont « particulièrement vulnérables aux divers impacts cérébraux du temps passé devant un écran. » [35]

4.2. L'intimidation (Bullying)

Les conclusions des GD d'enfants corroborent la littérature décrivant les différentes formes que prend l'intimidation en ligne, y compris la violence verbale, le discours de haine, la moquerie déguisée en plaisanteries, le sexisme, l'homophobie, le collorisme, le capacitisme et le body shaming. L'impact psychologique sur les victimes est sévère. Les participants des régions rurales et de l'intérieur ont exprimé leur vulnérabilité aux abus en ligne par des personnes des régions côtières ou de la capitale que les participants ont perçue comme les méprisant et les traitant de noms désobligeants en raison de leur région, de leur couleur de peau et de leurs accents.

Le harcèlement qui perpétue les clivages régionaux et socio-économiques, le sentiment de marginalisation et le fait d'être l'objet de mépris ont été expressément évoqués par les participants

31 Altevogt, B. M., Hanson, S. L., & Leshner, A. I. (2008). Autism and the Environment: Challenges and Opportunities for Research. Pediatrics. 121(6), 1225–1229. doi:10.1542/peds.2007-3000.
32 Begley, J. (2014) "Connect: the development of an online social network for people on the autism spectrum and their families". Good Autism Practice. 15: 2.
33 Howard, P. L., & Sedgewick, F. (2021) 'Anything but the phone!': Communication mode preferences in the autism community. Autism. 25:8, 2265-2278.
34 Pavlopoulou, G., Usher, C., & Pearson, A. (2022). 'I can actually do it without any help or someone watching over me all the time and giving me constant instruction': Autistic adolescent boys' perspectives on engagement in online video gaming. British Journal of Developmental Psychology, 40, 557-571. https://doi.org/10.1111/bjdp.12424
35 Dunckley, V.L. (2016). Autism and Screen Time: Special Brains, Special Risks: Children with autism are vulnerable to the negative effects of screen time. Psychology Today. https://www.psychologytoday.com/us/blog/mental-wealth/201612/autism-and-screen-time-special-brains-special-risks

aux FG à Tebourba, Gafsa et Kasserine. Kortli (17 ans, garçon) a noté que « les gens plus riches de la côte ou de la capitale utilisent des termes péjoratifs pour nous désigner, disant que nous sommes des classes inférieures, se moquant de notre accent et de notre teint ». Cela a un impact profond sur les participants, car Grappa (17 ans, garçon) a déclaré que ce type de traitement « vous donne l'impression que vous n'êtes personne » . De plus, les participants ont noté que l'intimidation avait un impact plus important sur les personnes ayant une faible estime de soi. Alors que les participants ont largement qualifié Facebook de plate-forme principale pour les messages négatifs et l'intimidation, d'autres plates-formes de médias sociaux, telles qu'Instagram et Tiktok, ont également été citées.

> « Les garçons de ma classe ont ce jeu où le garçon qui quitte la classe en dernier se fait gifler par tous les garçons. Ceci est ensuite publié en ligne pour que tout le monde puisse le voir. » (Garçon, 13 ans)

L'intimidation peut aussi inclure le body shaming, comme le rappelle la professeure principale émérite lors d'un entretien avec l'équipe de recherche, « il y avait une fille en surpoids dans l'école où j'enseignais. Ses camarades de classe ont posté une vidéo de son corps lui faisant honte. Cela a eu un impact négatif sur elle. La direction de l'école n'a réagi qu'en s'adressant aux coupables mais ils n'ont reçu aucune conséquence réelle de leurs actes » . En outre, cette recherche empirique corrobore également la littérature soulignant les liens intrinsèques entre la violence en ligne et hors ligne, car les enfants participants au GD ont mis en évidence des cas où l'intimidation et la violence hors ligne se déplacent en ligne et, à leur tour, perpétuent davantage la violence hors ligne. Par exemple, Swayah (13 ans, garçon) a déclaré que « les garçons de ma classe ont ce jeu où le garçon qui quitte la classe en dernier se fait gifler par tous les garçons. Ceci est ensuite publié en ligne pour que tout le monde puisse le voir. » Les participants ont convenu que cela a des impacts psychologiques et physiques car cela est humiliant pour la victime tout en perpétuant la violence du monde réel à son encontre. Comme Anatole (13 ans, garçon) l'a déclaré « vous deviendrez connu comme la personne que tout le monde peut frapper et vous intimider ». En plus de mettre en évidence les expériences d'intimidation des enfants, les résultats attirent également l'attention sur l'importance de mesures adéquates et appropriées prises par les écoles, et plus largement, en réponse à l'intimidation et à la cyberintimidation, pour protéger la victime et remédier au comportement de la part des harceleurs.

4.3. Le piratage (hacking)

Les participants ont fréquemment cité le piratage comme un risque. En particulier, leurs mots de passe peuvent être déterminés ou extraits par des « liens pirates », qui incitent les utilisateurs à cliquer dessus uniquement pour voler leurs mots de passe. Une fois qu'un pirate a accès à un compte, les participants ont noté le préjudice potentiel qui peut être causé à ses données personnelles et à sa réputation (si leurs comptes sont réquisitionnés). Fait important, les participants ont également exprimé leurs connaissances sur la façon de se protéger contre ces risques, mais ont admis qu'il devrait y avoir une meilleure prise de conscience du risque et de la nécessité de former les enfants sur la façon d'éviter le piratage, par exemple en évitant d'utiliser leur vrai nom lors de la création de comptes et de l'identification les signes d'un lien suspect.

4.4. Le harcèlement sexuel

Le harcèlement sexuel était un risque principalement lié au genre, les garçons interrogés déclarant ne pas être particulièrement touchés. D'autre part, les filles sont la cible de harcèlement sexuel en ligne, par le biais du « body shaming », de la réception de messages et de photos non sollicités, ou de la republication de leurs photos qu'elles avaient publiées sur les réseaux sociaux dans des groupes Facebook avec des légendes et des commentaires inappropriés. Comme Touta (17 ans, fille) l'a rapporté, elle a posté une photo de son visage sur sa page Facebook, pour la trouver sur une autre page FB avec une légende inappropriée à caractère sexuel. Les participants ont noté que la plupart des failles de sécurité et des contacts non sollicités qu'ils ont rencontrés se sont produits sur Facebook. Il convient de noter que, bien que les discussions sur le harcèlement sexuel aient principalement eu lieu dans les groupes de discussion réservés aux filles, les réponses au questionnaire d'enquête anonyme administré aux enfants à la fin de chaque groupe de discussion révèlent que la majorité de tous les répondants ont été victimes de rencontres sexuelles non désirées sur Internet. Sur les 108 enfants ayant répondu à la question « J'ai vu ou reçu un message, une photo ou une vidéo à caractère sexuel que je ne voulais pas recevoir », 66/108 ont répondu oui. Cela indique que 61 % des répondants ont été soumis à du contenu sexuel non sollicité (veuillez consulter le graphique ci-dessous).

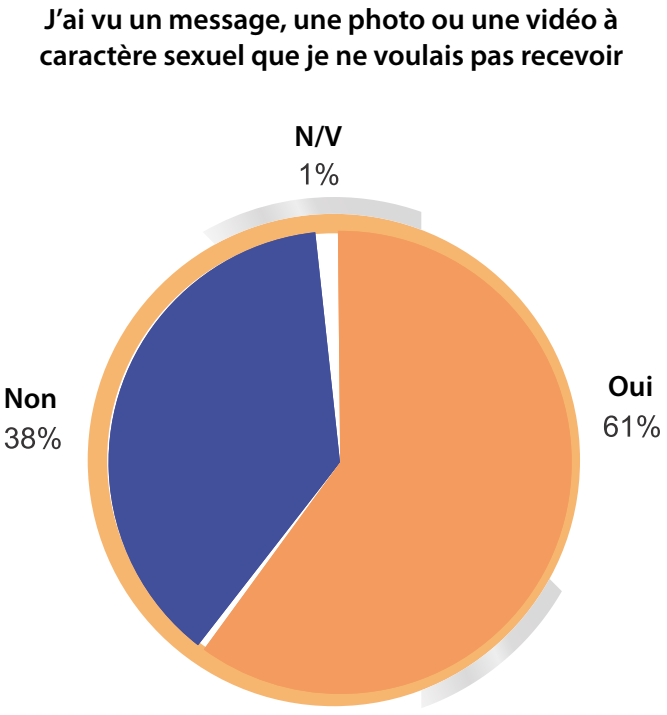

Figure 1: Réponses a la question 6 du questionnaire anonyme

De plus, 36 répondants ont fourni des réponses qualitatives à la question 19 de l'enquête : «J'ai eu de mauvaises expériences en ligne dont je ne voudrais parler à personne.» Il s'agit principalement de cas d'intimidation, de piratage (faux profils), d'images sexuelles non sollicitées, de harcèlement sexuel, d'abus d'image, de diffamation et d'extorsion (voir l'annexe 6 pour une liste complète des réponses à la question 19 de l'enquête).

4.5. Faux profils et extorsion

Les faux profils Facebook ont également été évoqués comme une menace majeure pour les filles sur Internet. Cela peut se produire lorsque quelqu'un utilise les photos de quelqu'un d'autre (qui pourraient être disponibles sur les réseaux sociaux) pour créer un profil prétendant être lui et envoyer des messages inappropriés à ses contacts et publier du contenu inapproprié. Les participants ont indiqué qu'ils connaissent de nombreuses personnes qui en ont été victimes, y compris certaines des participantes elles-mêmes. Cela entraîne des problèmes et la perte d'amitiés pour la victime.

Marceline (14 ans, fille) a rapporté que quelqu'un avait pris sa photo sur Facebook, avant de coller son visage sur des images explicites via le biais de Photoshop, puis avait ouvert un nouveau compte Facebook en se faisant passer pour elle. Lorsqu'elle a expliqué cette expérience pénible au groupe de discussion, elle a éclaté en sanglots. Notamment, Marceline a expliqué qu'elle l'avait rapporté à sa mère, car elle craignait d'autres problèmes potentiels. Cependant, sa mère, qui a participé à un GD de parents, n'a pas mentionné cet incident. Cela pourrait indiquer que la mère a choisi de ne pas parler publiquement de cette question, devant des chercheurs et des pairs. Cela pourrait également indiquer le déni parental de ces questions, peut-être en raison d'une éventuelle honte sociale : les parents sont réticents à signaler les cas d'extorsion avec de vraies ou de fausses photos par crainte de risques potentiels pour leur réputation.

En plus de causer du tort, les données des GD ont montré comment les faux profils Facebook facilitent l'extorsion. Les participants ont décrit comment cela se produit lorsqu'une personne assume une identité différente, généralement une femme, et se lie d'amitié avec ses victimes féminines sur les réseaux sociaux. Après avoir gagné leur confiance, l'agresseur peut convaincre la victime d'avoir des conversations vidéo avec eux et/ou de leur envoyer des photos intimes. L'agresseur fait ensuite chanter la victime avec ce matériel. Le chantage peut être de nature monétaire ou sexuelle. Plusieurs participantes ont déclaré que cela leur était arrivé, avec des impacts psychologiques dévastateurs et durables. Une participante de GD 5 a déclaré avoir été victime d'un faux profil, ce qui lui a valu un chantage pendant quatre ans.

Rihan (14 ans, fille) a partagé une histoire qu'elle a vécue deux ans avant le GD. Une (supposée) femme s'est liée d'amitié avec elle sur TikTok, puis a déplacé leurs conversations sur Facebook où elle a commencé à la convaincre d'envoyer des photos intimes d'elle-même. Elle a assuré à Rihan que « ça va parce que nous sommes toutes les deux des filles ». L'agresseur a également piégé Rihan en prenant des captures d'écran d'un appel vidéo initié par l'agresseur dans lequel Rihan était entièrement vêtu mais la personne à l'autre bout de la ligne était nue. Lorsque Rihan a finalement été convaincue d'envoyer des photos intimes d'elle-même, l'agresseur a commencé à la faire chanter et à essayer de contacter la famille de Rihan. L'impact psychologique est toujours clair sur Rihan, qui a fondu en larmes en racontant sa victimisation. Notamment, son histoire a incité d'autres participantes à se manifester, racontant leur victimisation dans des circonstances très similaires lorsqu'elles avaient 12 ans. En effet, Marceline a également fondu en larmes en déclarant « il m'est arrivé la même chose. » Kira (14) a également déclaré qu'une connaissance en ligne avait tenté de la convaincre d'envoyer des photos lorsqu'elle avait 12 ans. Kira, cependant, a démontré sa résilience en refusant puis en bloquant la personne.

Notamment, les victimes ont rapporté que les auteurs les avaient également amenées à cliquer sur des liens pornographiques ou à rechercher des actes sexuels. Cette recherche n'a trouvé aucune donnée systémique sur l'étendue de l'extorsion en ligne ou son impact sur les victimes. Cependant,

ce phénomène porte des tendances alarmantes, comme le note la pédopsychiatre Dr Fatma Charfi « nous rencontrons un nombre élevé de filles ayant des pensées suicidaires dues à l'extorsion (sexuelle) » (entretien avec l'équipe de recherche).

En plus de l'impact psychologique d'être victime de ces programmes, toutes les participantes ont montré un manque de connaissances sur où et comment obtenir de l'aide, et sur les droits légaux dans de telles situations. Cela renforce les conclusions du sondage U-Report 2020, qui a montré que seulement un enfant sur cinq savait où demander de l'aide s'il en avait besoin.[36] Lorsqu'elles ont été alertées sur le fait qu'elles pouvaient signaler ces crimes, elles ont toutes déclaré qu'elles ne voudraient pas signaler de peur d'être blâmés par leurs familles et la police. En effet, Rihan, qui a déclaré avoir finalement parlé à sa mère de ce qui lui était arrivé, a déclaré « jusqu'à présent, ma mère m'en veut et ne cesse de me blâmer. Je n'ai pas de bonnes relations avec ma mère à cause de cela. » En plus de la peur des réactions des familles, il existe une perception générale selon laquelle la police n'est pas utile dans ces situations. Comme l'a déclaré Nawel, « nous savons tous ce qui se passe dans les postes de police. Si vous allez là-bas pour dénoncer quelqu'un pour avoir menacé de partager des photos intimes de vous, ils vous reprocheront probablement d'avoir pris ces photos en premier lieu » (17 ans, fille). Il s'agit d'une constatation importante pour lutter contre le non-signalement et pour créer un système et un climat dans lesquels les enfants se sentent en sécurité pour signaler, et peuvent le faire sans crainte de représailles et de récrimination.

> « Nous savons tous ce qui se passe dans les commissariats. Si vous allez là-bas pour dénoncer quelqu'un pour avoir menacé de partager des photos intimes de vous, ils vous reprocheront probablement d'avoir pris ces photos en premier lieu » (Nawal, 17 ans, fille).

Tant les filles que les garçons ont convenu que les filles sont touchées de manière disproportionnées par les faux profils cherchant à extraire des photos et des vidéos à des fins d'extorsion. Tous les participants ont également convenu que les normes sociétales patriarcales signifient que les femmes et les filles sont tenues responsables lorsqu'elles sont victimes d'extorsion en raison des notions d'honneur associées au corps d'une fille. Comme Grappa a dit « si quelqu'un partage mes photos, personne ne s'en souciera parce que je suis un garçon » (17 ans, garçon). De plus, ces mêmes normes sociétales constituent un obstacle au signalement.

Cependant, les garçons sont victimes différemment des faux profils. Certains participants masculins ont révélé qu'ils connaissaient de nombreux amis qui avaient été attirés par un faux profil prétendant être une fille cherchant à se rencontrer en personne. Lorsque la victime se rend à la réunion en personne, elle se fait agresser par un homme ou un groupe d'hommes.

4.6. La banalisation de la violence et la radicalisation en ligne

Pour les participants au GD, les risques sont également liés au fait que les adolescents s'aventurent dans les côtés obscurs d'Internet, tels que le dark web, la pornographie et les «OnlyFans». Cela peut conduire à un « lavage de cerveau » des adolescents ou à des problèmes de personnalité et de comportement. Dans ce contexte, certains participants au GD ont indiqué avoir été exposés par inadvertance à des contenus très dérangeants et inappropriés sur les réseaux sociaux, comme un compte TikTok dédié à la publication de vidéos illustrant le meurtre et le démembrement de

36 UNICEF Tunisia (2020). Violence Against Children and Adolescents U-Report poll. Disponible à https://tunisie.ureport.in/opinion/4674/

personnes. Comme l'a déclaré Melissa, « J'ai vu une fois une vidéo de quelqu'un tuant et éventrant un petit enfant. Cela m'a vraiment affecté négativement pendant longtemps » (17 ans, fille, GD6).

De plus, les enfants participants au GD ont discuté des impacts durables potentiels de l'exposition à du matériel ou à des idéologies violentes sur les adolescents impressionnables. Bien que la banalisation de la violence par le biais de jeux et de vidéos ait été évoquée lors des discussions de groupe avec les enfants, les parents et les enseignants, ainsi que lors des entretiens avec les principales parties prenantes, celles-ci ont été largement discutées comme une forme de violence non intentionnelle (sans intention de nuire) qui affecte les enfants différemment. Cependant, d'autres formes de manipulation, plus intentionnelles, ont été soulevées, comme la radicalisation vers l'extrémisme religieux violent ou non violent. La juge pour enfants Asmahan Boudhrioua, spécialisée dans les affaires de lutte contre le terrorisme, a confirmé que « alors que la radicalisation des adultes se produit en grande partie hors ligne, comme à la mosquée, la plupart des enfants sont radicalisés sur les réseaux sociaux. Les premières phases de radicalisation se passent généralement sur Facebook puis on demande aux enfants de passer sur l'application plus sécurisée Telegram. »

4.7. Risques pour la santé mentale

Les participants ont discuté des diverses façons dont les expériences en ligne négatives peuvent avoir un impact sur leur santé mentale. Il a été largement noté que les messages négatifs, la pêche à la traîne et l'intimidation ont des effets néfastes sur leur estime de soi et leur santé mentale, ce qui a des effets sur la santé mentale un risque qui recoupe tous les autres risques évoqués ci-dessus. Les participants ont critiqué les « faux » modes de vie perpétués par les utilisateurs des médias sociaux prétendant être plus riches ou plus heureux qu'ils ne le sont réellement. Cela peut réduire leur estime de soi lorsqu'ils se comparent à des normes irréalisables. De plus, certaines participantes ont signalé que la « positivité toxique », perpétuée par les influenceurs sur les réseaux sociaux, nuit à la santé mentale des téléspectateurs, car elle les amène à avoir une image corporelle et des attentes de style de vie irréalistes. Bien qu'ils soient conscients que les modes de vie et les normes de beauté qu'ils rencontrent sur les réseaux sociaux sont « faux », les participants ont estimé que «si vous êtes exposé à ces 'stories' tous les jours, elles vous affecteront forcément négativement » (Souhir, 17 ans, fille). L'impact est une baisse de l'estime de soi car les enfants se comparent à des normes irréalisables.

> «Mentalement, nous sommes beaucoup plus âgés que notre âge parce que nous avons des problèmes auxquels nous ne devrions pas avoir à faire face à notre jeune âge.» (Mayar, 16 ans, fille)

Les participants ont discuté de l'impact négatif que les faux profils ont sur leurs relations avec leur famille et leurs amis. Dans un exemple particulièrement tragique, un participant a rapporté l'histoire d'une amie qui avait eu une relation en ligne avec quelqu'un pendant des années, mais qui s'est avéré être un faux profil. Le faux profil l'a ensuite fait chanter avec des photos et des vidéos. Cela a tellement affecté la victime qu'elle s'est suicidée.

En plus des préjudices d'extorsion susmentionnés, les obstacles rencontrés par les femmes et les filles les empêchant de signaler ou de discuter des crimes dont elles sont victimes ont également des effets négatifs sur la santé mentale. En effet, les participants conviennent que les normes sociétales patriarcales signifient que les femmes victimes seront blâmées et davantage victimisées

pour avoir été victimes de chantage avec des photos et des vidéos compromettantes. Cela signifie que la plupart des victimes ne se sentent pas suffisamment en sécurité pour discuter de ces problèmes avec leur famille ou pour les signaler aux autorités. Par conséquent, la victime continue de subir les crimes en silence, avec des impacts négatifs sur sa santé mentale. Comme l'a déclaré Mayar, « mentalement, nous sommes beaucoup plus âgés que notre âge parce que nous avons des problèmes auxquels nous ne devrions pas avoir à faire face à notre jeune âge » (16, fille, GD5).

III. Prévention et réponse aux risques et préjudices en ligne auxquels sont confrontés les enfants

Alors que tous les enfants participants ont rapporté des expériences à la fois positives et négatives lors de l'utilisation d'Internet, les discussions de groupe ont révélé un niveau élevé de sensibilisation et d'action parmi les enfants, qui se considéraient largement comme détenant le pouvoir de récolter les bénéfices d'Internet tout en mettant en place des mesures pour prévenir ou répondre à tous les risques et préjudices.

1. Approches existantes des enfants en matière de protection en ligne

La majorité des enfants participants au GD ont démontré une connaissance des types d'informations personnelles disponibles à leur sujet sur Internet, y compris leurs noms, âge, sexe, amis, choses qu'ils aiment et n'aiment pas, comptes de messagerie, lieux qu'ils visitent et où ils vivent, leur visage et leurs photos, leurs familles et où ils vont à l'école. Comme l'a résumé un participant au GD 6, « Internet sait tout de nous ! » (Rose, 17 ans, fille).

« Internet sait tout de nous ! » (Rose, 17 ans, fille).

1.1. Mesures actives prises par les enfants pour se protéger en ligne

Parmi les enfants FG, les participants ont discuté de diverses mesures qu'ils ont mises en place pour se protéger, notamment la création d'un compte Facebook sécurisé, la rétention de leurs informations réelles sur les réseaux sociaux, y compris leur âge réel et leur adresse personnelle, le fait de ne pas autoriser les applications à accéder à leurs données, de ne pas accepter les personnes qu'ils ne connaissent pas sur les réseaux sociaux, en gardant leurs photos privées et en signalant tout profil ou contenu suspect. Par exemple, comme l'ont plaisanté les participants au GD 2, ils sont des experts pour identifier les signes révélateurs d'un faux profil Facebook, comme une photo de profil fortement filtrée et irréaliste, très peu de « J'aime » sur les photos et les publications, et un compte très récent avec un petit nombre « d'amis ». Cette vigilance est ensuite suivie d'actions pour prévenir les risques, notamment le blocage et le signalement des comptes suspects. Certaines des réponses des enfants au questionnaire d'enquête anonyme dans lequel ils racontaient des rencontres négatives sur Internet incluaient également les mesures qu'ils avaient prises pour répondre ou se protéger, telles que « vous pouvez résoudre ces problèmes en ne répondant pas ou en bloquant les gens » ou « je l'ai dit à ma mère et elle comprenait heureusement. » Après avoir

relaté un cas où il/elle a été incité par un faux profil à envoyer des photos intimes d'eux-mêmes, un enfant a écrit : « j'ai refusé et je l'ai supprimé de ma liste d'amis ». Cependant, la fréquence à laquelle les enfants signalaient également des escroqueries et étaient eux-mêmes trompés par de faux profils, dans la discussion sur les risques et les méfaits, suggère que dans la pratique, de nombreux enfants ne sont pas aussi entraînés et aptes à repérer et à éviter les faux profils Facebook qu'ils le pourraient se croient être.

> « Parfois, je me fais un devoir d'utiliser toutes mes données 3G sur mon téléphone pour ne plus être tentée d'aller en ligne ». (Arin, 17 ans, fille).

De même, les participants, principalement des filles, ont volontairement mis en place des mesures concrètes pour modérer eux-mêmes leur utilisation d'Internet pendant l'année scolaire, notamment en limitant les jeux aux vacances d'été. D'autres ont eu recours à des mesures non conventionnelles pour limiter leur utilisation d'Internet. Comme l'a déclaré une participante du GD 8, « parfois, je me fais un devoir d'utiliser toutes mes données 3G sur mon téléphone pour ne plus être tentée d'aller en ligne » (Arin, 17 ans, fille). Dans les GDs, les enfants participants ont reconnu qu'une utilisation excessive d'Internet peut être évitée en s'engageant dans des activités et des passe-temps parascolaires et de plein air. Cela a été corroboré par le fait que les participants qui se livraient à de telles activités, telles que le sport ou la musique, passaient le moins de temps en ligne.

Cependant, ces activités ne sont souvent pas disponibles ou possibles pour tous les enfants, en particulier pour les enfants issus de milieux socio-économiques moins favorisés. De plus, le temps que les enfants du groupe d'âge cible passent à l'école ou dans des séances de tutorat est systématiquement considéré par les enfants et les parents comme privant les enfants du temps et de l'énergie pour toute activité parascolaire. Comme Chahad, participante au FG, l'a illustré : « je termine l'école à 18 heures plusieurs jours, puis j'ai deux heures de tutorat en dehors de l'école, puis je dois rentrer chez moi et faire mes devoirs » (13 ans, fille, GD13). Le résultat est que les enfants sont tellement épuisés mentalement et physiquement que « si j'en ai fini avec les activités scolaires à 21 heures, tout ce dont j'ai l'énergie, c'est de parcourir Facebook pendant quelques heures au lit » (Maria, 17 ans, fille, GD8).

1.2. La recherche d'aide et de soutien

Notamment, la majorité des enfants ont déclaré compter sur le soutien de leurs amis et pairs dans les cas où ils sont exposés à des risques et à des préjudices en ligne, plutôt que de discuter de leurs problèmes avec leurs parents. Cela est conforme à la littérature examinée dans l'analyse documentaire (annexe 1) qui révèle que les enfants recherchent en grande partie l'aide ou les connaissances de leurs pairs plutôt que de leurs parents. Cela pourrait être attribué au « fossé numérique » perçu et réel entre les parents et les enfants, en plus du manque de dialogue ouvert et sans jugement à la maison. En effet, « dans tous les pays, le rythme rapide de l'innovation technologique sape la compétence parentale, ce qui, à son tour, sape la volonté des enfants de se tourner vers leurs parents pour obtenir de l'aide. »[37]

37 Livingstone & Byrne (2018) p.19

1.3. Des mesures de protection adaptées et différenciées

En outre, les participants ont reconnu que les risques en ligne n'affectent pas les enfants de la même manière ni dans la même mesure. Certains participants aux groupes de discussion ont souligné certains facteurs sous-jacents qui rendent certains enfants plus vulnérables que d'autres à des risques particuliers. Les participants au GD 8 ont souligné que les impacts négatifs de l'intimidation et d'autres expériences négatives sur Internet sont réduits chez les personnes ayant une plus grande estime de soi, ce qui rend nécessaire de cultiver la résilience des enfants en améliorant la confiance en soi. Cela a été corroboré dans un entretien avec la pédopsychiatre, le Dr Ahlem Belhadj, qui a affirmé que « tout ce qui peut nuire à un enfant en ligne n'est pas une forme de violence. Par exemple, le phénomène des influenceurs en ligne est très négatif, mais son impact varie selon les enfants en fonction de leurs personnalités, de leurs expériences vécues, de leur environnement familial. C'est généralement un enfant vulnérable qui est le plus touché négativement ».

Comme l'ont fait valoir les enfants participants aux GD, si les utilisateurs souffrent d'une faible estime de soi ou sont vulnérables aux expériences négatives en ligne, ils peuvent mettre en place d'autres mesures préventives, comme éviter les interactions sur les réseaux sociaux afin d'éviter de lire des messages négatifs. Dans l'ensemble, les enfants des groupes de discussion ont également souligné la responsabilité des utilisateurs d'éviter et de signaler les vidéos inappropriées, telles que les contenus incitant à la violence ou à la haine. Dans le même ordre d'idées, les participants ont recommandé de suivre les personnes positives sur les réseaux sociaux.

> IL EST À NOTER QUE LES ENFANTS CONSIDÉRAIENT PRINCIPALEMENT COMME LEUR PROPRE RESPONSABILITÉ DE RESTER EN SÉCURITÉ EN LIGNE, PLUTÔT QUE DE COMPRENDRE LES LIMITES DE LEUR PROPRE RESPONSABILITÉ, ET DE RECONNAÎTRE OÙ LA RESPONSABILITÉ PASSAIT À D'AUTRES, ET EN PARTICULIER, AUX DÉVELOPPEURS D'APPLICATIONS, AUX PLATEFORMES DE MÉDIAS SOCIAUX ET AUTRES AU SEIN DU SECTEUR DES TECHNOLOGIES NUMÉRIQUES.

La majorité des participants ont convenu que le contrôle parental est nécessaire pour les jeunes enfants de moins de 13 ans. Par exemple, en réponse à l'exposition à des contenus indésirables et à des publicités à caractère sexuel en ligne, un garçon de 13 ans participant au GD 16 a pensé que « j'aimerais que ma mère m'enlève mon téléphone, pour que je n'aie plus à voir ces choses » (Antonio, garçon). En effet, dans les FG d'enfants, les participants ont souligné la nécessité pour les parents et la famille de limiter l'utilisation d'Internet pour les jeunes enfants et de surveiller les sites Web et les contenus auxquels ils sont exposés.

Les groupes de discussion ont révélé un niveau général de sensibilisation et d'action parmi les enfants participants pour mettre en œuvre des mesures préventives et réactives pour faire face aux risques et aux méfaits en ligne d'une part, et un retard concomitant dans la connaissance et la compréhension parmi les parents des avantages, des risques et des mesures en ligne pour la prévention et la réponse d'autre part. En outre, les données des entretiens avec les principales parties prenantes ont révélé plusieurs exemples actuels ou antérieurs d'initiatives gouvernementales et non gouvernementales positives pour la prévention et la réponse à la violence en ligne. Celles-ci sont explorées ci-dessous, en vue de tirer les leçons et des recommandations pour éclairer le plan d'action national.

2. Efforts et mesures existants pour la prévention et la réponse

Un certain nombre d'initiatives et de projets ont été mis en œuvre par diverses institutions gouvernementales tunisiennes, des organisations de la société civile et avec le financement et le soutien de donateurs internationaux et d'ONG pour sensibiliser les enfants et les parents à la sécurité sur Internet. Par exemple, dans un entretien avec M. Lotfi Belazi, directeur général du Centre national de l'informatique pour l'enfant (CNIPE) , il a décrit les initiatives de sensibilisation passées et prévues de son centre. Il a souligné que la sensibilisation des enfants est un axe central pour le centre, recoupant toutes leurs offres de cours. Comme l'a déclaré M. Belazi, « quant à la sensibilisation et la prise de conscience, ce sont des outils présents dans toutes les unités ». Le centre veille à équilibrer la sensibilisation des enfants aux risques et méfaits liés à Internet avec une appréciation de ses bienfaits (voir encadré) : « nous lui montrons le côté positif. Et quand il arrive à positiver, il y a le côté de prise de conscience et de sensibilisation [...]. Et il faut savoir qu'il y a un mauvais côté, à savoir que si tu partages tes données, d'autres personnes peuvent l'utiliser, qu'il existe des gens qui sont à l'affut de ces choses-là, qu'il existe aussi des réseaux de pédophilie, etc » .

> IL EST IMPORTANT QUE TOUTES LES INITIATIVES DE SENSIBILISATION, ET CELLES VISANT À FAVORISER LE CHANGEMENT SOCIAL ET COMPORTEMENTAL, ÉQUILIBRENT UNE CONSCIENCE DES RISQUES EXISTANT EN LIGNE POUR LES ENFANTS ET LES MESURES PRISES POUR LES PROTÉGER, AVEC UNE CONSCIENCE ÉGALE DES BÉNÉFICES ET DES OPPORTUNITÉS EN LIGNE POUR LES ENFANTS. CELA A ÉTÉ EXPRIMÉ PAR LE DIRECTEUR GÉNÉRAL DU CENTRE NATIONAL DE L'INFORMATIQUE POUR L'ENFANT, QUI NOTE : « NOUS LUI MONTRONS LE CÔTÉ POSITIF. ET QUAND IL ARRIVE A POSITIVER, IL Y A LE CÔTÉ DE PRISE DE CONSCIENCE ET DE SENSIBILISATION [...]. ET IL FAUT SAVOIR QU'IL Y A UN MAUVAIS COTE, A SAVOIR QUE SI TU PARTAGES TES DONNEES, D'AUTRES PERSONNES PEUVENT L'UTILISER, QU'IL EXISTE DES GENS QUI SONT A L'AFFUT DE CES CHOSES-LA, QU'IL EXISTE AUSSI DES RÉSEAUX DE PÉDOPHILIE, ETC .»

Des entretiens avec d'autres parties prenantes clés ont révélé des exemples réussis de coordination et de collaboration interinstitutionnelles pour sensibiliser les enfants et les parents aux risques et à la sécurité d'Internet. Par exemple, M. Anis Aounallah, Délègue à la protection de l'enfance de Tunis, a rappelé une campagne de sensibilisation qui a été mise en œuvre avec succès entre son bureau et le CNIPE.[38] De même, M. Hichem Chebbi, inspecteur général au sein du ministère de l'Education a confirmé que son ministère a un partenariat établi avec le CNIPE et ses 24 centres régionaux à travers tous les gouvernorats tunisiens. Comme l'a expliqué M. Chebbi, les élèves du primaire et du collège sont encouragés par leurs écoles à visiter le CNIPE ou ses affiliés régionaux pour recevoir une gamme de cours de TIC, de programmation et de robotique. « Les enfants de l'école primaire et des collèges, tu les retrouves là-bas. Y en a qui y vont tout seuls et y en a qui y vont via les écoles ». Cependant, il convient de noter que les centres régionaux sont situés dans les centres du gouvernorat et sont donc inaccessibles aux enfants issus de milieux ruraux et éloignés. De plus, comme l'a admis M. Belazi, « les Centres Nationaux d'Informatique ou les Centres Régionaux, ne sont pas assez présents sur le territoire et n'ont pas les services ou un plan de communication pour les faire connaître au public, que ce soit chez les parents ou chez les enfants ».

38 Le CNIPE est un établissement public à caractère administratif jouissant de l'autonomie administrative et financière sous la tutelle du MFFES

En plus des initiatives menées par le gouvernement, la société civile et les ONG ont également mis en œuvre des projets de sensibilisation. Par exemple, l'Association «Sawn» de protection des enfants et des adolescents contre la violence et les abus sexuels organise des ateliers de sensibilisation ciblant les enfants et leurs parents pour les sensibiliser et améliorer la communication enfants-parents sur les questions liées aux abus sexuels, y compris ceux perpétrés ou diffusés en ligne. Comme l'a expliqué la présidente de Sawn, Mme Faouzia Chaabane Jabeur, ces ateliers visent à briser ce sujet tabou en « expliquant aux parents ce que sont les signes d'abus sexuels et comment ils peuvent en parler avec leurs enfants ». En outre, des entretiens ont révélé une initiative antérieure entreprise par l'UNICEF en 2015 pour sensibiliser les enfants, les parents, les éducateurs et les médecins à la violence sexuelle contre les enfants. Cette initiative a été abandonnée suite à son adoption par le ministère de la Santé, en raison du manque de ressources et du manque de coordination entre les ministères.

Des entretiens avec des parties prenantes clés ont révélé qu'en plus de la sensibilisation, un autre facteur important de prévention consiste à renforcer la résilience des enfants face aux risques et aux méfaits en ligne en cultivant des « compétences générales » ou des « compétences de vie ». Le directeur général du CNIPE, M. Belazi, considère l'avancement des compétences non techniques, ou les Soft Skills des enfants comme « un enjeu stratégique qui concerne la réforme de la société, et la restructuration de la société dans son ensemble ! Parce que les « soft skills » pour nous, c'est aider les enfants à développer des compétences de vie »

Cette approche est progressivement intégrée dans le système éducatif. Comme l'a expliqué M. Chebbi, inspecteur général au sein du ministère de l'Éducation, le ministère est dans les dernières phases de conception d'un programme transversal et holistique axé sur l'amélioration des compétences de vie des enfants dans les deux premières années de l'enseignement primaire. Selon M. Chebbi, « l'éducation à la santé globale a pour but de protéger l'enfant de toutes sortes d'agressions sexuelles. La prise de décision est Parmi les compétences sur lesquelles on travaille et qui est très importante.». Par exemple, le nouveau programme prévoit de présenter aux enfants des situations fictives pour mesurer leur niveau de compréhension du consentement et leur apprendre les types de situations qui les justifient pour refuser la collaboration et parler à leurs parents. Notamment, ce programme, intitulé «santé globale», est un reconditionnement d'une précédente initiative proposée par le ministère intitulée «santé sexuelle» dont le déploiement a été écourté en raison d'un contrecoup sociétal. En effet, du fait du « branding » initial du programme « ça a fait une polémique insensée. Les parents ont pensé qu'on allait apprendre le sexe aux enfants ». Cela suggère que la sensibilisation des parents, associée à une stratégie de communication améliorée, est nécessaire pour la réussite de la mise en œuvre réussi de ces initiatives.

En plus des pratiques existantes liées à la prévention mentionnée ci-dessus, cette recherche a révélé un certain nombre d'initiatives positives pour la réponse et la prise en charge des victimes. Par exemple, le Conseil de l'Europe a financé la création du centre « injed » en 2016, la première Unité Médico-Judiciaire qui accueille les femmes et les enfants victimes d'abus sexuels.[39] Le centre est un guichet unique, un centre de style Barnahuse [40] qui peut fournir un bureau adapté aux enfants, sous un même toit, où les forces de l'ordre, la justice pénale, les services de protection de l'enfance et les travailleurs médicaux et de santé mentale coopèrent dans l'évaluation de la situation des enfant et la prise de décision.

39 C'est dans cette unité que sont réalisés les examens médicaux exigés par les autorités judiciaires pour prouver la culpabilité de l'agresseur.
40 Terme scandinave pour « maison d'enfants ». Veuillez consulter ce lien pour plus de détails..

Le Conseil de l'Europe a également fourni un financement à l'Instance nationale de lutte contre la traite des personnes pour développer une boîte à outils pour la détection et la prise en charge des victimes de la traite des êtres humains, y compris les enfants.

En l'absence de financement, les acteurs impliqués dans la protection de l'enfance ont également utilisé leur propre initiative pour fournir une prise en charge efficace aux victimes. Par exemple, malgré l'absence de programmes de déradicalisation ou de soutien aux enfants, la juge pour enfants, Mme Asmahan Boudhrioua, a trouvé un moyen créatif de traiter les cas impliquant des enfants radicalisés en ligne. Comme elle l'a expliqué, « nous avons dans le code de protection de l'enfance une institution juridique abandonnée « liberté surveillée. » J'ai utilisé le mécanisme de la liberté surveillée pour instaurer un programme de déradicalisation en collaboration avec d'autres partenaires bénévoles ».Ce processus comprenait une évaluation du degré de radicalisation de l'enfant, un suivi psychologique, un accompagnement pour reprendre des études ou intégrer une formation professionnelle en coordination avec le DPE et en étroite collaboration avec la famille. Ces efforts se sont avérés fructueux. En trois ans d'application de cette démarche, « on avait zéro cas de récidive, et aucun enfant n'a de nouveau participé à un dossier terroriste » .

3. Lacunes juridiques et institutionnelles dans la prévention et la réponse à la violence en ligne

La cartographie du cadre juridique tunisien (annexe 2) a démontré l'existence de plusieurs textes législatifs qui traitent la question de la violence en ligne contre les enfants, d'une façon directe ou indirecte. Ces textes abordent la question sous différents angles revêtant un caractère sectoriel. En effet, il n'existe pas actuellement un texte juridique qui traite la question d'une façon holistique liant entre la protection de l'enfance d'une part et la violence en ligne d'une autre part. Ainsi, les dispositions relatives à la violence contre les enfants en lignes sont éparpillées sur plusieurs textes:

- Les textes relatifs à la violence contre les enfants (le code pénal, le code de la protection de l'enfance, Loi organique n°58 - 2017 du 22 août 6027 relative à l'élimination de la violence faite aux femmes, La loi organique n°61 de 2016 du 3 août 2016 sur la prévention et la lutte contre la traite des personnes, La loi organique n° 26 de 2015 du 7 août 2015 relative à la lutte contre le terrorisme et de prévention du blanchiment d'argent) ;
- Les textes relatifs à l'information/communication (La loi n° 1 de 2001 du 15 janvier 2001 portant promulgation du code des télécommunications, la loi n°63 de 2004 du 27 juillet 2004 relative à la protection des données personnelles, le décret-loi n 115 - 2011 du 2 novembre 2011 relatif à la liberté de la presse, Décret-loi n° 2022-54 du 13 septembre 2022, relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication).

La fragmentation de la législation portant sur différents aspects de l'OPCSEA à travers les secteurs et les actes contribue en partie au manque fragmenté et parfois simple d'application et de mise en œuvre appropriées des dispositions juridiques et politiques existantes, bien que ce soit davantage le manque de mise en œuvre des lois existantes qui ont été identifiés par de nombreuses parties prenantes comme responsables des goulots d'étranglement et des lacunes dans la fourniture de services aux victimes de la violence en ligne.

3.1. Des lacunes juridiques

L'absence d'un texte juridique spécifique traitant de la violence en ligne contre les enfants n'a pas été considérée comme un problème inhérent par la plupart des principales parties prenantes interrogées. Comme l'a déclaré M. Aounallah, DPE de Tunis, « la violence contre les enfants est codifiée dans la loi, quel que soit le moyen par lequel cette violence est perpétrée. En ce sens, la réponse à la violence en ligne contre les enfants ne diffère pas de la réponse à toute forme de violence contre les enfants ». De même, Mme Raoudha Bayoudh, représentante du ministère de l'Intérieur au sein de l'Instance nationale de lutte contre la traite des personnes (INLTP) a fait valoir que « le problème n'est pas juridique. Quel que soit le vide juridique qui existait en matière de violence en ligne, il a été comblé par le Décret-loi n° 2022-54 relatif à la cybercriminalité ».

Dans le même ordre d'idées, les juges de la famille et des enfants interrogés dans le cadre de cette recherche ont estimé qu'ils disposaient de la base juridique nécessaire pour traiter les cas de violence en ligne, tels que l'extorsion, tant pour les enfants victimes que pour les enfants auteurs. Comme l'a expliqué la juge pour enfants Mme. Asmahen Boudhrioua, juge de troisième grade à la cour d'appel, « les articles 218 et 219 du code pénal criminalisent la violence physique, puis la loi 58 est venue élargir la définition de la violence à la violence psychologique. »En outre, alors que la loi 58 est essentiellement axée sur la violence basée sur le genre, « la pratique judiciaire a jusqu'à présent appliqué cette loi au profit des enfants, même dans les cas où la violence basée sur le genre n'existe pas ». Cependant, cela « dépend des efforts et de la jurisprudence de chaque juge dans l'application de la loi ». De même, la juge de la famille Mme. Sonia Jeridi a déclaré dans un entretien avec l'équipe de recherche que « le principe de l'intérêt supérieur de l'enfant est la formule magique utilisée par les juges pour tirer parti des outils juridiques existants au profit de l'enfant » . En outre, comme l'a souligné le juge pour enfants Mme. Boudhrioua, « les conventions internationales dont la Tunisie est signataire, comme la convention de Lanzarote, sont contraignantes et peuvent être utilisées par les juges dans les affaires de violences sexuelles ». Par exemple, avant la loi 58, le juge Mme. Boudhrioua appliquait la convention de Lanzarote pour garantir que les enfants victimes de violences sexuelles ne soient interrogés qu'une seule fois en présence d'un psychologue.

Notamment, et en raison du recours à la jurisprudence des juges, il est important de souligner le manque de formation spécialisée pour les juges de la famille et des enfants sur la protection de l'enfance. Comme l'a souligné le juge pour enfants Mme. Boudhrioua, « les juges ne choisissent pas leur nomination mais sont souvent déplacés de différents endroits pour devenir juge de la famille ou juge des enfants. Lorsque je suis devenu juge des enfants, je n'ai reçu aucune formation spécialisée. Je ne connais la convention de Lanzarote que parce que j'ai fait des recherches et j'ai reçu une formation de l'UNICEF entre 2012 et 2014 » .

De plus, les principaux intervenants interrogés conviennent que le code de protection de l'enfance est désuet et doit être modifié pour inclure la notion de victime. Comme l'a expliqué M. Aounallah, DPE de Tunis, « il y a une différence entre un enfant victime et un enfant en situation de menace, donc les réponses doivent être différentes ». Ceci est important car, comme le révèle l'analyse documentaire, les victimes de violence en ligne courent un plus grand risque de devenir elles-mêmes des auteurs de violence. Comme l'a rappelé le juge de la famille, Mme. Jediri, « il y a eu un cas où un garçon extorquait une fille de son école. La victime a subi des séquelles psychologiques et j'ai donc ordonné un suivi psychologique pour elle. Cependant, il était également clair que l'enfant agresseur avait également des problèmes émotionnels (...). Notre système judiciaire considère ce garçon

comme un auteur, mais j'ai également ordonné un suivi psychologique pour lui ». Cela souligne la nécessité d'une identification et d'une réponse efficaces aux enfants victimes, afin de prévenir de futures violences. Comme l'a soutenu le juge pour enfants, Mme. Boudhrioua, « généralement, un enfant en conflit avec la loi est un enfant victime qui a reçu une prise en charge insuffisante. »

Comme l'ont confirmé les principales parties prenantes interrogées, des efforts ont été déployés pour modifier le code de protection de l'enfance afin d'y inclure un chapitre sur les « enfants victimes et témoins ». Cependant, ce processus est au point mort depuis des années et, en raison de l'instabilité politique persistante et de l'absence actuelle d'un organe législatif, on ne sait pas quand ce processus pourra être achevé. En outre, alors que le contexte de la protection de l'enfance en Tunisie bénéficie désormais de lois plus avancées, telles que la loi 58 et la loi 61, celles-ci ont créé des problèmes pratiques car les outils et le mandat à la disposition du DPE en vertu du code de la protection de l'enfance sont devenus inadéquats. Par exemple, comme l'a expliqué M. Aounallah, DPE de Tunis, « en vertu du code, j'étais le premier point de contact pour les enfants victimes d'abus sexuels. Cependant, désormais la loi 58 stipule que les unités de police spécialisées doivent être contactées et que l'audition de l'enfant ne peut avoir lieu qu'une seule fois en présence d'un psychologue ou d'un travailleur social. Cela signifie que, désormais, si je reçois un signalement concernant un enfant victime d'abus sexuels, je n'ai légalement pas le droit de l'écouter ».

Nonobstant les lacunes juridiques, les données des entretiens ont également révélé un accord général entre les principales parties prenantes sur une lacune dans la mise en œuvre du cadre juridique existant. Cet écart peut être attribué à un ensemble de facteurs, chacun décrit dans la sous-section ci-dessous.

Orientations mondiales sur la législation pour l'OCSEA

Des lignes directrices récemment publiées sur légiférer pour l'ère numérique reconnaissent la nature en évolution rapide de l'environnement numérique et les défis qu'il présente pour une législation efficace. Cependant, il présente six domaines qui doivent au minimum être intégrés dans les codes juridiques nationaux :

- Criminalisation de l'OCSEA et application de ces lois
- De nouvelles procédures d'investigation, de stockage, de conservation et de conservation des preuves électroniques,
- Régulation des entreprises dans l'environnement numérique
- Services de protection de l'enfance pour les victimes d'OCSEA,
- L'accès à la réparation pour les enfants victimes, et
- Surveillance indépendante des droits des enfants à la protection dans l'environnement numérique.

Les Lignes directrices demandent explicitement, entre autres, l'inclusion d'une définition complète des abus et de l'exploitation sexuels des enfants, y compris lorsqu'ils sont facilités par l'utilisation des TIC, et des dispositions garantissant que les adolescents ne doivent pas être criminalisés pour des actes consensuels et non exploitant activités sexuelles, et qu'un enfant ne devrait pas être tenu responsable de la génération, de la possession ou du partage volontaire et consensuel de son propre contenu sexuel, uniquement pour un usage privé. Les lignes directrices proposent également

l'inclusion d'autres infractions spécifiques à l'OCSEA telles que le cyberflashing, le cyberharcèlement ou l'upskirting. Aucun de ces aspects n'est actuellement codifié dans le cadre législatif tunisien. . (United Nations Children's Fund (2022) 'Legislating for the digital age: Global guide on improving legislative frameworks to protect children from online sexual exploitation and abuse' UNICEF, New York.)

3.2. Lacunes dans les connaissances et les capacités des principaux acteurs de la protection de l'enfance

Manque de connaissances et de capacité de signalement chez les acteurs clés : Cette recherche a révélé un manque général de connaissance parmi les acteurs concernés de l'obligation de signaler les suspicions de maltraitance d'enfants, et de l'anonymat de ce signalement, tel que stipulé par l'article 31 du code de protection de l'enfance. Les résultats des groupes de discussion avec les enseignants ont révélé leur manque de connaissances sur cette obligation. De plus, lorsque les enseignants étaient conscients de cette obligation, ils montraient une réticence à signaler, par crainte de harcèlement ou de représailles de la part de l'auteur de l'abus ou de la famille de l'enfant. Ces craintes par les enseignants et autres professionnels peuvent être perçues ou réelles. Comme l'a déclaré M. Mihyar Hamadi, le Délégué général à la protection de l'enfance (DGPE), il y a eu des cas d'enseignants qui ont été victimes de harcèlement après avoir signalé des abus : « il y a eu un cas dans lequel une enseignante a signalé des abus potentiels sur un enfant. La famille de l'enfant a déposé une plainte auprès de la police contre l'enseignante pour diffamation. L'enseignante a ensuite été convoquée au poste de police et nous avons dû expliquer à la police que l'enseignante ne faisait que remplir son obligation légale de signaler les cas présumés de maltraitance d'enfants ». Cela suggère que des efforts supplémentaires sont nécessaires pour accroître les connaissances des éducateurs et des principaux acteurs de la protection de l'enfance sur les mécanismes de signalement obligatoires et de réponse. Comme l'a déclaré M. Aounallah, DPE de Tunis, « malgré la diffusion par le ministère de l'Éducation de multiples notes à son personnel sur le signalement obligatoire, ces notes ne parviennent pas aux enseignants, en particulier dans les zones reculées ». Comme l'a indiqué M. Hamadi, DGPE, il existe un protocole d'accord entre le ministère de l'Éducation et le MFFES. Dans le cadre de ce partenariat, la « DPE a proposé de former les éducateurs et le personnel administratif des établissements scolaires à l'obligation et à la démarche de signalement des cas potentiels de maltraitance ». Cependant, au moment de la rédaction du présent rapport, le DPE n'a pas reçu de réponse.

L'amélioration des connaissances et des capacités des éducateurs sur les mécanismes de signalement et de réponse doit être associée à une sensibilisation accrue du public, y compris des enfants et des parents, aux risques et à la sécurité en ligne, en plus des garanties et mécanismes juridiques existants en cas de victimisation d'enfants. De telles initiatives de sensibilisation peuvent simultanément contribuer aux efforts de prévention ainsi qu'à l'identification et à la réponse à la violence existante.

Le signalement obligatoire (et non obligatoire) de la violence en ligne, associé à un manque de sensibilisation et de compréhension de ce qui constitue les différentes formes de violence en ligne, ne présente qu'un obstacle à la prestation efficace de services aux victimes de l'OCSEA et d'autres formes de violence en ligne. L'absence de toute orientation ou protocole, intégré dans le système de gestion des cas, pour le signalement de l'OCSEA, au-delà des infractions déjà couvertes

par les directives de signalement obligatoires (qui ne reconnaissent pas explicitement la violence facilitée par la technologie, ou les voies de signalement ou d'orientation des victimes de différentes formes d'exploitation et d'abus sexuels d'enfants en ligne). L'incorporation de capacités et d'options explicites pour faire face à l'OCSEA et à d'autres formes de violence en ligne dans le système formel de protection de l'enfance est encore compliquée par l'absence de définitions juridiques très claires des différentes formes de violence facilitée par la technologie et des mesures spécifiques à prendre. en réponse à chacun. Bien que l'application des lois existantes puisse dans certains cas être utilisée, le manque de définitions juridiques existantes très claires entrave probablement davantage une réponse pratique centrée sur l'enfant et adaptée aux victimes par le système de protection de l'enfance.

Un fossé technique et numérique entre les acteurs de protection de l'enfance : Comme l'a souligné M. Aounallah, DPE de Tunis, « il est particulièrement difficile de tracer les criminels en ligne, surtout s'ils utilisent un faux profil ». Mme Bayoudh, représentante du ministère de l'Intérieur au sein de l'INLTP précise en outre que « la collecte des preuves nécessaires à la condamnation est la chose la plus difficile dans les cybercrimes. C'est souvent compliqué si la victime supprime la preuve parce qu'elle a peur, ou si le suspect supprime la preuve ou utilise un faux profil, ou si le suspect est hors de Tunisie, surtout compte tenu des problèmes de coordination que nous avons avec Interpol ». Ces efforts peuvent être encore entravés par le manque de culture numérique parmi les acteurs gouvernementaux. Par exemple, M. Aounallah a déclaré que « de nombreux acteurs gouvernementaux n'ont pas la capacité de base pour utiliser les technologies numériques. Auparavant, je ne savais pas que si quelqu'un m'envoyait des preuves vidéo de maltraitance d'enfants sur Facebook, je devrais les télécharger immédiatement sur mon téléphone. J'ai appris cela à mes dépens lorsqu'une vidéo qui m'a été envoyée a été supprimée à la source et que j'ai perdu la preuve. J'ai dû apprendre par moi-même à gérer ces technologies » . Cela reflète le manque général d'intégration des outils numériques dans l'administration. Par exemple, comme l'a expliqué M. Aounallah, « de nombreuses institutions gouvernementales utilisent encore le fax. J'ai parfois dû envoyer des photos par fax, et quand elles arrivent, elles sont sombres et impossibles à discerner ».

Cela démontre un manque de compréhension quant à la manière dont les preuves, ou les preuves potentielles, d'exploitation et abus sexuels d'enfants en ligne doivent être traitées de manière à protéger les droits de la victime et à garantir la viabilité des preuves dans le cadre des poursuites et des procédures judiciaires. Par exemple, le téléchargement et le stockage de Matériel d'exploitation sexuelle d'enfants par le personnel de protection de première ligne, ou par toute personne extérieure à l'unité de cybercriminalité, peuvent augmenter les chances que davantage de personnes voient le matériel, ou perdent ou volent des données et du contenu, et finalement, compromettent la confidentialité et la protection de la victime.

Par conséquent, la nature technique de la violence en ligne nécessite une refonte des capacités numériques humaines et matérielles pour assurer une réponse efficace. Comme l'a souligné Mme Bayoudh, représentante du ministère de l'Intérieur au sein de l'INLTP, « la nouvelle loi sur la cybercriminalité est venue combler le vide juridique dans la lutte contre la criminalité en ligne. En théorie, nous avons des institutions telles que l'Agence Tunisienne d'Internet et des unités spécialisées au sein du ministère de l'Intérieur pour faire face à la cybercriminalité. En pratique, ces acteurs manquent de moyens techniques pour lutter efficacement contre ces délits hautement techniques. »

3.3. Manque de soutien psychologique pour les enfants

Les enfants participants aux groupes de discussion ont constamment souligné leur besoin d'accéder à un soutien psychologique. Cependant, les données des entretiens ont révélé une lacune dans la fourniture d'un soutien psychologique aux enfants et aux victimes de violence. Selon la majorité des acteurs clés interrogés, le nombre de psychologues au sein des ministères de la Santé, de l'Education et des Affaires Sociales est insuffisant. En outre, comme l'a déclaré la pédopsychiatre, Dr Fatma Charfi, « le nombre de psychologues affiliés au ministère de la Santé pourrait être suffisant s'ils étaient répartis de manière efficace. Par exemple, le ministère a affecté des psychologues aux urgences. Cependant, ces psychologues pourraient être mieux utilisés ailleurs où il y a un besoin plus pressant ».

En revanche, les structures conçues pour apporter un soutien psychologique aux enfants scolarisés, telles que les bureaux d'écoute et de conseil (BEC)[41] et les cellules d'écoute et de conseil (CEC) [42] créées par le ministère de la Santé, n'ont effectivement jamais fonctionné en raison de l'indisponibilité des psychologues. En conséquence, comme l'a souligné Mme Faouzia Chaabane, présidente de l'organisation de la société civile « Sawn », « on est allé travailler à Hay Hlel, à Mallesin, à Sidi Hsin, et à chaque fois, on trouvait des jeunes et des parents dans les écoles, complètement perdus et à la recherche de psychologues. »

En outre, comme l'a expliqué M. Aounallah, DPE de Tunis, les psychologues affiliés au gouvernement sont en grande partie confinés à leurs bureaux et ne font pas de visites sur le terrain, dans les écoles ou dans les domiciles. Cela a été corroboré par Mme. Chaabane, qui a souligné que « les psychologues qui travaillent au ministère de l'Éducation et dans les délégations se déplacent rarement aux écoles. Alors que normalement ils devaient être en contact avec les enfants et non pas avec les délégations. Le psychologue doit être présent avec les jeunes, ça n'est pas un travail administratif ». Le manque de psychologues va souvent à l'encontre de l'objectif d'initiatives telles que le centre « Injed », qui visent à s'aligner sur la stipulation de la convention de Lanzarote et la loi 58 exigeant que les enfants victimes d'abus sexuels ne soient interrogés qu'une seule fois en présence d'un psychologue. En outre, comme l'a souligné M. Aounallah, « le manque de soutien psychologique est particulièrement important dans la prise en charge des enfants qui ont été radicalisés. On a toujours du mal à trouver des psychologues formés et capables de s'occuper de ces enfants » .

Alors que les restrictions financières peuvent empêcher le recrutement de personnel psychologique supplémentaire aux ministères de la Santé, des Affaires Sociales, de l'Education et du MFFES, cette recherche a révélé que la coordination avec la société civile peut aider à combler ce fossé. Par exemple, comme l'a expliqué M. Aounallah, DPE de Tunis, « nous avons travaillé avec certaines OSC, telles que les Psychologues du Monde et Health and Psychology, en particulier lorsque nous devons identifier des psychologues qui sont disposés et capables de se déplacer ». Cependant, comme l'a déclaré M. Aounallah, travailler avec des acteurs de la société civile peut être difficile lorsque leurs efforts de collecte de fonds conduisent à une violation de la confidentialité. Par exemple, « j'ai collaboré une fois avec une organisation de la société civile sur un cas d'abus, puis j'ai découvert qu'ils publiaient toutes nos communications et les spécificités du cas en ligne dans le cadre de leurs efforts pour attirer des financements ».

41 Ce sont des permanences au sein des écoles préparatoires et des lycées secondaires assurées par le conseiller d'information et d'orientation, le médecin scolaire de l'établissement et le travailleur social de l'établissement.
42 Ce sont des permanences médicales au sein des établissements secondaires ou supérieurs assurées par les médecins scolaires.

Les recommandations avancées dans la section suivante de ce rapport sont basées sur les pratiques et initiatives existantes et sur les meilleures pratiques mondiales, en plus des lacunes identifiées dans cette section. Ce processus de recherche a révélé qu'une stratégie efficace pour lutter contre la violence en ligne contre les enfants doit se concentrer sur la prévention ainsi que sur la réponse.

IV. Recommandations

Le nombre croissant des études et de preuves, ainsi que les orientations mondiales, sur ce qui fonctionne pour prévenir et répondre à la violence en ligne contre les enfants, fournit un cadre utile pour la manière dont les conclusions de cette recherche peuvent éclairer des recommandations pratiques, réalistes et réalisables. Les recommandations ci-dessous s'appuient en particulier sur les stratégies INSPIRE pour mettre fin à la violence contre les enfants, ainsi que sur le modèle de réponse nationale MNR (discuté en détail dans la revue de la littérature), pour assurer l'alignement de la réponse avec les engagements et stratégies mondiaux et régionaux - une considération particulièrement importante pour la protection dans l'environnement numérique, qui, par définition, transcende les frontières nationales et nécessite une coopération et une collaboration mondiales et régionales. Les recommandations ci-dessous fournissent également un point de départ pour l'élaboration du plan d'action national d'une manière qui évite les chevauchements et la duplication des efforts. Ainsi, pour chaque recommandation, ce rapport identifie les domaines potentiels de synergies avec les stratégies et les efforts gouvernementaux ou non gouvernementaux existants.

Il est essentiel de veiller à ce que la voix des enfants soit au cœur de l'élaboration de toutes les politiques et législations ayant un impact sur les enfants dans l'espace numérique. Étant donné l'intersection entre la sécurité et le bien-être des enfants en ligne et tous les autres aspects de leur vie dans l'espace numérique, tels que l'apprentissage, le jeu et la participation civique, la centralité des voix et des expériences des enfants doit être assurée dans tous ces secteurs pour créer un environnement fondé sur les droits afin de garantir et améliorer la protection des enfants en ligne.

1. Recommandations sur la recherche et les données

Souvent considérées comme une priorité secondaire pour l'élaboration des politiques et la législation, une recherche de qualité et des données de bonne qualité sont essentielles pour une bonne élaboration des politiques et des législations et la conception d'interventions appropriées et bien conçues. Pour cette raison, ces recommandations sont soulignées en premier.

Une base de référence quantitative, fiable et représentative des expériences, à la fois positives et négatives, des expériences en ligne, des opportunités, des compétences et des méfaits pour tous les enfants en Tunisie, devrait être établie. Cette étude a mis en évidence l'importance de consultation avec les enfants ainsi que l'importance de disposer de données fiables et représentatives sur les expériences des enfants utilisant Internet et la technologie numérique. Bien que cette étude soit de nature qualitative et ne soit pas représentative de tous les enfants en Tunisie, elle donne un aperçu de certaines des préoccupations, lacunes et priorités existantes pour assurer la sécurité des enfants, ainsi que certains des défis institutionnels et structurels.

La disposition de données quantitative permettra de disposer de données de référence pour éclairer le suivi du Plan d'Action National sur la protection en ligne des enfants, ainsi que pour éclairer la conception d'interventions appropriées. La prochaine étude Disrupting Harm (DH)[43] offre une occasion concrète de le faire.

Bien que Disrupting Harm offre la possibilité de collecter et d'utiliser les données représentatives nécessaires pour mieux surveiller et mettre en œuvre la législation, les politiques et les programmes, il sera important de veiller à ce que des données qualitatives plus détaillées, telles que celles collectées dans cette étude, soient collectées à intervalles réguliers pour fournir la nuance et la profondeur aux données quantitatives recueillies par DH. En particulier, une meilleure compréhension des perceptions des enfants sur la confidentialité et la protection des données est nécessaire afin de mieux évaluer comment les enfants partagent des informations, quelle connaissance ils ont de la vie privée et quelles mesures ils prennent pour mieux se protéger et protéger leurs données, ainsi que leurs informations personnelles, en ligne. Il est important que ces données soient collectées directement auprès des enfants, plutôt qu'auprès des parents, car l'opinion des parents sur la compréhension de la vie privée et de la protection des enfants est souvent dichotomique par rapport à celle des enfants eux-mêmes. Il est également important de comprendre de la perception des parents sur qu'ils pensent savoir des activités, risques, etc. de leurs enfants en ligne.

De même, à mesure que l'EdTech et d'autres utilisations de la technologie numérique dans les salles de classe se déploient plus largement en Tunisie, davantage de recherches seront nécessaires sur les mesures et les mécanismes que les écoles prennent pour protéger les enfants en ligne, pour doter les enfants des compétences et capacités dont ils ont besoin, et de protéger leurs données.

La collecte de données et le suivi régulier doivent être intégrés aux processus de collecte de données administratives de routine, tels que les données scolaires et le passage à un système de gestion intégré au sein du système de protection de l'enfance, qui permet d'enregistrer et signaler tous les problèmes liés à l'utilisation de la technologie par les enfants.

Certaines étapes positives sont déjà en cours vers la collecte de données liées à la violence en ligne. Par exemple, comme l'a indiqué M. Anis Aounallah, DPE de Tunis, « le nouveau site Web du DPE en préparation, où les cas de violence contre les enfants peuvent être signalés, désagrège les moyens par lesquels cette violence est perpétrée ». Cela peut être encore renforcé par d'autres organes liés au MFFES, tels que l'observatoire des droits de l'enfant. À terme, il est nécessaire que le MFFES élabore et mette en œuvre un programme de recherche portant sur les violences en ligne faites aux enfants et des recommandations politiques et législatives.

Un certain niveau de réforme législative est nécessaire pour atteindre le niveau de conformité et de cohérence législative envisagé (et requis) pour lutter contre la violence sexuelle et d'autres formes de violence en ligne dans le cadre des droits de l'enfant envisagé dans le MNR et d'autres cadres mondiaux. La Tunisie occupe une position enviable dans la région en raison de son engagement déclaré et de son historique de priorisation des droits de l'enfant dans son cadre législatif et politique, et cela peut être mis à profit pour développer davantage les meilleures pratiques régionales.

43 Disrupting Harm est un projet de recherche mené dans 14 pays en partenariat entre UNICEF, ECPAT International et INTERPOL, financé par le Partenariat mondial pour mettre fin à la violence contre les enfants. Le projet a été créé pour générer des preuves de haute qualité sur l'exploitation et la maltraitance sexuelles facilitées par la technologie.

1.1. Garantir la cohérence entre les instruments et les lois

La législation doit être révisée et, si nécessaire, modifiée, pour assurer la cohérence entre les instruments et les lois, ainsi que la cohérence avec les orientations et connaissances législatives les plus récentes. La cohérence est nécessaire dans l'ensemble de la législation afin de garantir des normes communes aux différents acteurs dans le cadre de la protection, de l'application de la loi et de la réponse judiciaire à la violence en ligne, et, dans la mesure du possible, d'éviter le pouvoir discrétionnaire des juges et des procureurs. Bien que cela puisse présenter des avantages, cela peut également entraîner l'application de normes et de recours inégaux selon les individus concernés. L'application de normes communes, de définitions et d'une législation cohérente minimise ce risque. Plusieurs répondants à l'étude ont noté la pertinence de la loi existante, dans le contexte d'une application judicieuse, mais ont également noté la nécessité d'une réforme (voir ci-dessous). Le recours actuel à la discrétion des juges a été mis en évidence.

Cette recherche a révélé que le rôle et les outils dont dispose le DPE, tels qu'ils sont inscrits dans le Code de la protection de l'enfance, ne sont plus compatibles avec les exigences des textes législatifs plus récents tels que la loi 58 et la loi 61. Par exemple, comme le souligne M. Aounallah, DPE de Tunis « selon la loi 58 sur les violences basées sur le genre, la déclaration d'un enfant victime d'exploitation ou d'abus sexuels ne doit être recueillie qu'une seule fois en présence d'un psychologue ou d'un travailleur social. Cela signifie que, bien qu'il soit de mon devoir d'assurer la liaison avec les enfants et leur famille en vertu du code de protection de l'enfant, en vertu de la loi 58, si un enfant ou sa famille vient me voir pour signaler un abus sexuel, je ne suis pas autorisé à prendre leur déclaration. »

Il est donc nécessaire de revoir les mécanismes de la réponse et de la prise en charge compte tenu du nouveau paysage législatif, afin de surmonter les confusions et chevauchements procéduraux et de réaffirmer le rôle du DPE en tant que point de contact avec les enfants. En outre, une application cohérente et équitable des lois et politiques existantes doit être appliquée, et des mécanismes de responsabilisation doivent être formulés lorsque ce n'est pas le cas.

La mise en œuvre cohérente et efficace des lois relatives à la violence en ligne est aussi importante que la garantie d'un cadre législatif complet. Il a été récemment noté que « l'application de la loi et les mesures réglementaires peuvent avoir plus d'influence que la législation elle-même.» [44]

Il est de notoriété publique que la législation n'est efficace que dans la mesure où elle est mise en œuvre, et l'accent devrait être mis autant sur l'équipement de tous les acteurs responsables pour qu'ils prennent les mesures prescrites pour prévenir et répondre à toutes les formes de violence affectant les enfants dans l'espace numérique. Plusieurs personnes interrogées en Tunisie ont noté que le cadre législatif existant était adéquat, mais que son application était incohérente et parfois inexistante. Il est important que des mécanismes de responsabilisation soient mis en place pour garantir que, lorsque la loi n'est pas appliquée de manière appropriée ou adéquate, les victimes disposent d'une certaine forme de recours, et que les organismes gouvernementaux soient tenus responsables de la mise en œuvre des lois et réglementations. Cela pourrait être fait par l'introduction d'un médiateur, ou simplement par l'intégration d'indicateurs de performance clés qui intègrent des procédures, une gestion et une surveillance efficaces, et des sanctions claires lorsque celles-ci ne sont pas respectées.

44 WHO, 2022. pg. 10

1.2. Donner la priorité à la réforme du Code de la Protection de l'Enfance

Il est nécessaire d'introduire la notion d'enfant victime dans le cadre juridique existant relatif à la protection de l'enfance. S'il est difficile de surmonter l'instabilité politique qui a joué un rôle dans le ralentissement de ce processus, il est important de relancer ce processus et d'inclure la société civile dans les consultations liées à l'ajout d'un troisième chapitre au code relatif aux enfants victimes et témoins. Plusieurs considérations spécifiques doivent être intégrées, entre autres :

- Assurer la protection des enfants victimes qui peuvent être criminalisés lorsque le contenu auto-généré est partagé de manière non consensuelle, en tant qu'abus sexuel basé sur l'image.
- Assurer des recours pour les enfants victimes d'exploitation et d'abus sexuels en ligne.

Ce processus relève du mandat du MFFES en tant qu'agence chef de file, mais afin d'assurer une réponse coordonnée du système de protection, il est important d'impliquer, au minimum, la société civile, le ministère de l'Éducation, le ministère de la Justice, le ministère de l'Intérieur (l'Unité de la cybercriminalité), le ministère de la Santé, le ministère des Télécommunications, ainsi que le prochain organe législatif et le bureau du Premier ministre pour assurer la priorisation de cette réforme.

Meilleures pratiques en matière de protection des enfants en ligne en Australie, au Ghana et au Cambodge

En Australie, la loi sur la sécurité en ligne oblige tout fournisseur de services en ligne, des sociétés de médias sociaux et des fournisseurs de services Internet, à prendre des mesures raisonnables pour assurer la sécurité des enfants en ligne, notamment en répondant dans les 24 heures aux demandes d'ordres de retrait de CSAM, en répondant aux signalements de cyberintimidation ou d'autres risques. Ne pas le faire peut entraîner des sanctions civiles ou d'autres sanctions. Des dispositions prévoyant des sanctions et des amendes pour les fournisseurs de services de télécommunication qui ne prennent pas les mesures adéquates pour assurer la sécurité des enfants en ligne ont également été incorporées dans la législation récente du Ghana, par le biais de la loi sur la cybersécurité de 2020. Une autre alternative actuellement explorée au Cambodge est l'incorporation de mesures similaires dans les accords de licence pour les fournisseurs de services TIC et numériques. Le non-respect de ces obligations entraînerait le retrait des licences d'exploitation ou l'imposition de sanctions.

1.3. Établir des lignes directrices de l'industrie pour la protection des enfants en ligne

Une approche commune et équitable de la protection en ligne des enfants pour l'industrie de la technologie numérique et des TIC, accompagnée de lignes directrices pour l'industrie, doit être établie, afin de garantir le respect de leurs obligations d'assurer la sécurité des enfants en ligne et de prendre les mesures appropriées pour prévenir et répondre aux menaces en ligne. Ces lignes directrices doivent s'appliquer aux entreprises tunisiennes et internationales et doivent être conformes aux meilleures pratiques mondiales. Elles doivent prendre en compte des mesures telles que la sécurité et la confidentialité dès la conception, le contenu adapté à l'âge, la vérification de l'âge

et d'autres développements émergents et récents liés à l'industrie pour remplir leurs obligations de protection des enfants (voir encadré à droite). Ces obligations doivent être élaborées en consultation et avec l'accord des fournisseurs de services Internet et des organismes connexes en Tunisie.

2. Renforcement des capacités et des systèmes

Le besoin de renforcement des capacités et de formation sur la protection en ligne des enfants, les droits de l'enfant tels qu'ils se traduisent dans l'espace numérique et, dans certains cas, sur les compétences numériques, ressort constamment dans le cadre de cette recherche. Toutes les formations recommandées ci-dessous pourraient être accréditées auprès d'organismes sectoriels pertinents dans le cadre de développement professionnel, augmentant ainsi l'incitation pour les participants. Trois groupes cibles distincts ont été identifiés pour la formation :

2.1. Formation pour les éducateurs et les enseignants

Plusieurs domaines nécessitant un renforcement des capacités ont été identifiés, notamment une compréhension de l'éventail des droits de l'enfant qui peuvent être réalisés en ligne, la nécessité d'une compréhension plus nuancée et complète des risques auxquels les enfants sont confrontés (y compris ceux qui peuvent être présentés par l'utilisation croissante de la technologie numérique en classe (via EdTech) et les problèmes de confidentialité, les dommages potentiels, les droits effectifs et les stratégies fondées sur des preuves, et dans certains cas des compétences numériques plus complètes.

Les initiatives existantes comprennent les bureaux d'écoute et de conseil (BEC) et les cellules d'écoute et de conseil (CEC), mais une formation est également nécessaire pour améliorer la capacité des enseignants à identifier les signes de détresse et de traumatisme chez les enfants, et sur le signalement de la violence et l'exploitation et l'abus en ligne lorsqu'ils en prennent connaissance. En outre, en vue de combler le fossé entre le soutien psychosocial disponible, les capacités et les ressources pour les enfants, en particulier en dehors de Tunis, certains éducateurs peuvent recevoir une formation spécialisée et une qualification pour agir en tant que conseiller ou premier point de contact avec les enfants en recherche d'un soutien psychologique ou émotionnel.

Cette formation est de plus en plus importante à mesure que le ministère de l'Éducation, avec d'autres partenaires, déploie des projets pilotes et d'autres essais d'utilisation des tablettes dans les salles de classe. La sécurité numérique et la citoyenneté de base, ainsi que les compétences en matière de confidentialité et de protection des données, doivent faire partie de tout renforcement des capacités sur l'adoption et l'utilisation de ces nouvelles technologies en classe.[45]

45 Des conseils utiles sur l'utilisation d'EdTech peuvent être trouvés dans les nouvelles directives de l'UNICEF ici : United Nations Children's Fund, 'Child Protection in Digital Education: Policy Brief', UNICEF, New York, January 2023. http://www.unicef.org/documents/child-protection-digital-education

2.2.Formation des juges des enfants et de la famille

En raison du rôle central qu'ils jouent dans l'interprétation du cadre juridique pour l'intérêt supérieur de l'enfant, les juges des enfants et de la famille doivent recevoir une formation spécialisée avant leur nomination, ainsi que périodiquement, y compris sur les conventions internationales dont la Tunisie est signataire.

2.3. Formation à la littératie numérique pour les fonctionnaires publics

Cela nécessitera un changement culturel et matériel dans toutes les institutions gouvernementales tunisiennes pour numériser les archives et les communications. Cependant, les efforts de numérisation existants sont de nature sectorielle, tels que les donateurs de la réforme du secteur de la sécurité (tels que l'USIP et le PNUD) fournissant des équipements et une formation au ministère de l'Intérieur pour améliorer la numérisation. Aux fins du présent Plan d'Action National, et en vue d'avancer des objectifs réalistes, cette recommandation met l'accent sur l'amélioration de la culture numérique des DPE et des autres acteurs clés impliqués dans la protection de l'enfance.

Cependant, une lacune est particulièrement ressortie de l'étude et mérite une mention particulière. Cela concerne les compétences requises et les procédures impliquées, lorsque des signalements sont effectués ou lorsque des abus sexuels sur des enfants ou d'autres contenus numériques impliquant des enfants sont identifiés. Un protocole très explicite (avec formation) est nécessaire pour régir la gestion du contenu de manière à minimiser les vues et à rationaliser le flux de signalements et de contenu à travers le système juridique et de protection de l'enfance. Cela inclut comment et quand le contenu doit être téléchargé. En général, l'unité de lutte contre la cybercriminalité en Tunisie, devrait être la seule agence mandatée chargée de s'occuper de tout contenu illégal, plutôt que d'autres acteurs au sein des services de protection de l'enfance, qu'ils soient de première ligne ou administratifs. Ceci est également important pour la conservation et le traitement des preuves. Il s'agit à la fois d'une lacune en matière de formation et d'une lacune procédurale et protocolaire, car il n'y a pas d'orientations claires dont les responsables soient conscients pour déterminer la gestion du contenu inapproprié ou d'autres contenus préjudiciables. Cette lacune compromet probablement le potentiel de réussite de toute poursuite dans des affaires impliquant un contenu ou un comportement illégal, et compromet le potentiel de protections nécessaires à fournir aux victimes (y compris les protections relatives à la vie privée et à la confidentialité, ainsi que la revictimisation et la traumatisation secondaire qui peuvent se produire lorsque le contenu sexuel, en particulier d'un enfant, est vu inutilement par ceux qui ont un devoir de diligence). Il est important que tous ceux qui ont un devoir de diligence, des agents de protection de première ligne aux éducateurs, soient conscients des processus de signalement et des restrictions sur leur propre manipulation et visualisation des documents et devraient donc être un élément cohérent de toute formation, pas seulement pour les enfants mais également pour les travailleurs de la protection ou les fonctionnaires de l'administration publique.

UN PROTOCOLE EXPLICITE (AVEC FORMATION) EST NÉCESSAIRE QUI RÉGIT LE TRAITEMENT DU CONTENU DE MANIÈRE À MINIMISER LES VUES ET À RATIONALISER LE FLUX DES RAPPORTS ET DU CONTENU À TRAVERS LE SYSTÈME JURIDIQUE ET DE PROTECTION DE L'ENFANCE. CELA INCLUT COMMENT ET QUAND LE CONTENU DOIT ÊTRE TÉLÉCHARGÉ. EN GÉNÉRAL, L'ORGANISME D'APPLICATION DE LA LOI RESPONSABLE, EN TUNISIE L'UNITÉ DE CYBERCRIMINALITÉ, DEVRAIT ÊTRE LE SEUL AGENCE MANDATÉE RESPONSABLE DE S'ENGAGER AVEC TOUT CONTENU ILLÉGAL, PLUTÔT QUE D'AUTRES AU SEIN DES SERVICES DE PROTECTION DE L'ENFANCE, SOIT DE PREMIÈRE LIGNE OU ADMINISTRATIF

2.4. Formation sur le reportage responsable axé sur les droits de l'enfant pour les journalistes

Le processus de validation de ce rapport a mis en évidence l'importance des reportages responsables et axés sur les droits de l'enfant par les médias sur les expériences, les risques et les préjudices en ligne des enfants. Étant donné que ces histoires peuvent façonner le récit public, cela suggère la nécessité de former les journalistes à la manière responsable de rendre compte des enfants dans les informations. En effet, la manière dont les enfants subissent les risques et les préjudices en ligne, y compris le signalement d'incidents spécifiques, peut à la fois porter atteinte au droit des victimes à la vie privée et à la protection contre d'autres préjudices, et servir de véhicule à la désinformation. En Afrique du Sud, Media Monitoring Africa a développé une formation accréditée et non accréditée pour les journalistes en milieu de carrière sur le reportage responsable centré sur l'enfant, qui pourrait servir de modèle pour une formation similaire en Tunisie.[46] Ceci est en outre soutenu par un groupe de référence pour enfants qui surveille et commente régulièrement les reportages des médias impliquant des enfants.

2.5. Mécanismes de prévention et de réponse

Les recommandations relatives aux services d'intervention et de prévention portent sur trois domaines interdépendants : le changement social et comportemental, intégrant la sensibilisation et l'éducation à la prévention, le soutien aux parents, aux tuteurs, et aux enfants eux-mêmes, et le renforcement du système de protection de l'enfance avec un accent particulier sur les services psychosociaux pour les enfants.

2.6. Lancer des campagnes de sensibilisation ciblant les enfants et les parents

Les parents et les enfants en Tunisie sont conscients de bon nombre des risques auxquels les enfants peuvent être confrontés en ligne. Les attitudes et la sensibilisation des adultes ont tendance à se concentrer davantage sur les risques et les méfaits que la technologie numérique présente pour les enfants. Un plus grand investissement dans la sensibilisation et les programmes de changement social et comportemental (SBC) qui incluent la sécurité en ligne et la protection en ligne des enfants est nécessaire.

46 Media Monitoring Africa (2022) Empowering Children in the Media. Children Youth and Media. https://mediamonitoringafrica.org/empowering-children-in-media/

Il s'agit notamment de programmes de sensibilisation universelle, mais aussi de stratégies de changement social et comportemental plus ciblées ciblant certains des moteurs et facteurs de risque connus de la violence en ligne. Les résultats de cette recherche reflètent bon nombre des idées fausses fondées sur la peur et des messages incorrects qui sont souvent diffusés dans une tentative bien intentionnée de protéger les enfants. La prise de conscience de messages communs (et non fondés) par les parents et les enfants peut saper les actions, les connaissances et la prise de décision requises par les enfants pour rester en sécurité en ligne, ainsi que les actions entreprises par les parents et les tuteurs pour soutenir leurs enfants (tout en les équipant avec les compétences requises pour tirer le meilleur parti d'Internet).

La sensibilisation devrait cibler les enfants, les parents et les enseignants et viser à prévenir la violence en ligne grâce à une sensibilisation aux risques et à la sécurité d'Internet et au rôle des parents dans le contrôle et le soutien. En outre, les campagnes de sensibilisation doivent contribuer aux efforts de réponse par la sensibilisation aux garanties juridiques et aux mécanismes de soutien aux victimes. En fin de compte, ces campagnes de sensibilisation devraient chercher à briser les tabous et les obstacles au signalement de l'extorsion et du harcèlement sexuel, tout en renforçant une culture de dialogue ouvert et sûr entre parents et enfants.

Les parents et les enseignants doivent être sensibilisés à la multitude d'opportunités et d'avantages qu'offre Internet aux enfants, ainsi qu'à l'importance d'Internet et de la technologie numérique pour réaliser l'éventail des droits dont disposent les enfants. La recherche a révélé une bien plus grande prise de conscience des risques et des préjudices potentiels auxquels sont confrontés les enfants en ligne, avec une prise de conscience très limitée de la multitude d'avantages. La sensibilisation doit essayer d'éviter les messages basés sur la peur, dont il a été démontré qu'ils ne donnent aucun résultat positif et qu'ils sont inefficaces.

Parallèlement, un soutien ciblé aux parents et aux tuteurs, y compris de la naissance à l'âge adulte, devrait être fourni. Les preuves montrent de plus en plus l'importance de soutenir les parents et les tuteurs de très jeunes enfants, dans la meilleure façon de soutenir leurs enfants lorsqu'ils commencent à s'engager avec la technologie numérique. Cela va de la manière dont les enfants d'âges différents peuvent mieux utiliser la technologie numérique, du type d'activités adaptées à différents âges, du temps passé en ligne à différentes activités et de la manière dont la technologie numérique, lorsqu'elle est utilisée de manière appropriée à différents âges, peut aider et favoriser le développement et les compétences.

L'intégration de la littératie numérique de base, de la parentalité numérique et des compétences en matière de sécurité dans les programmes de développement de la petite enfance et de parentalité peut apporter des avantages substantiels aux enfants et aux parents.[47] Les initiatives existantes en partenariat avec le gouvernement tunisien offrent des opportunités d'intégrer la sécurité numérique dans la programmation existante avec un investissement supplémentaire minimal et offrant un résultat coût-bénéfice favorable. Un exemple est le partenariat de développement de la petite enfance existant entre l'UNICEF et le gouvernement tunisien pour piloter la programmation de développement de la petite enfance dans quatre sites.

47 Il est important de faire la différence entre la littératie numérique, la littératie médiatique et la sécurité en ligne. L'objectif de chacun est différent et chaque ensemble de compétences nécessite des compétences différentes, bien qu'elles puissent se chevaucher. Il faut veiller à ne pas réduire la sécurité en ligne aux interventions de littératie numérique, par exemple. Ceci est discuté plus en détail dans Finkelhor D, Walsh K, Jones L, Mitchell K, Collier A. Youth Internet Safety Education: Aligning Programs With the Evidence Base. Trauma Violence Abuse. 2021 Dec;22(5):1233-1247.

Un avantage supplémentaire de l'intégration des messages de sécurité en ligne dans de telles initiatives est la possibilité d'atteindre les travailleurs sociaux ou de protection de l'enfance de première ligne ainsi que les parents ou les soignants.

En Tunisie, les initiatives prévues pour intégrer la messagerie de développement de la petite enfance dans les centres mère-enfant gérés par le ministère de la Santé offrent également des gains faciles pour diffuser et sensibiliser et informer sur la meilleure façon dont les parents peuvent soutenir leurs enfants, ainsi que pour diffuser des messages fondés sur des preuves plutôt que des messages ad-hoc non étayés par des preuves auxquelles les parents pourraient autrement être exposés. Une telle approche offre également la possibilité de diffuser des informations sur la recherche d'aide et le signalement de l'exploitation sexuelle ou d'autres formes d'abus qui pourraient autrement être plus difficiles à cibler sur les soignants.

Il existe également des preuves provenant d'ailleurs dans le monde que l'éducation à la prévention et la sensibilisation peuvent donner des résultats positifs dans la prévention de la violence en ligne, tant du point de vue de la victime que de l'auteur. De même, compte tenu de l'intersection entre les facteurs de violence à l'égard des enfants et la violence en ligne à l'égard des enfants, il est fort probable que les interventions pour la prévention de la violence à l'égard des enfants produiront des résultats positifs similaires pour la violence en ligne. L'adaptation d'interventions et de programmes fondés sur des données probantes qui se sont avérés efficaces pour intégrer des éléments de protection en ligne produiront des résultats positifs similaires en matière de sécurité en ligne.

2.7. Améliorer la résilience des enfants face aux risques et préjudices en ligne

En Tunisie, cela peut impliquer l'incorporation d'un programme scolaire plus large et d'une programmation extrascolaire qui se concentre sur les relations respectueuses, l'empathie, la bonne prise de décision, la résolution des conflits et la communication, favorisant finalement une plus grande résilience des enfants. Au sein de la région MENA, ces sujets sont abordés à travers l'éducation aux compétences de vie et à la citoyenneté (ECVS). Conceptuellement, le ECVS vise à doter les enfants et les jeunes d'un ensemble de compétences à travers différentes dimensions, au niveau individuel, social et instrumental. Le sujet s'appuie sur la notion de quatre groupes de compétences essentielles à la croissance et au développement: compétences pour l'apprentissage, compétences pour l'autonomisation personnelle, compétences pour la citoyenneté active et compétences pour l'employabilité. Au sein de chacun de ces ensembles de compétences se trouvent des « compétences essentielles pour la vie ». Tous ces éléments ont une incidence directe sur la sécurité en ligne. Les compétences d'apprentissage comprennent généralement la créativité, la pensée critique et la résolution de problèmes; les compétences pour l'employabilité incluent la négociation, la résolution des conflits et la coopération, et les compétences pour une citoyenneté active incluent le respect de la diversité, l'empathie et la participation, et les compétences pour le développement personnel incluent l'autogestion, la résilience et la communication. Chacun de ces ensembles de compétences est évident dans la plupart des programmes de prévention de la violence chez les jeunes et les enfants fondés sur des données probantes, même si ce n'est pas encore le cas dans les programmes ciblant les violences en ligne.[48]

48 Voir UNICEF Middle East and North Africa. 2017. Analytical mapping of life skills and citizen education in the Middle East and North Africa. Life Skills and Citizenship Education Initiative. UNICEF MENA: Jordan. Disponible à https://www.unicef.org/mena/reports/analytical-mapping-life-skills-and-citizenship-education-mena

Cette recherche a trouvé des preuves de programmes et d'initiatives gouvernementaux existants, quoique naissants, axés sur l'amélioration de la résilience des enfants, sur lesquels on peut s'appuyer, comme l'initiative de programme santé globale et les offres du CNIPE. Notamment, comme le révèle ce rapport de recherche, il est important pour le CNIPE et ses centres régionaux d'améliorer leur portée et leur visibilité par la conception et le lancement d'une stratégie de communication. En fin de compte, des centres similaires devraient être lancés en dehors des centres des gouvernorats pour faciliter l'accès aux enfants des zones rurales et reculées. La sensibilisation peut également s'appuyer sur les initiatives existantes du ministère de l'Éducation, du ministère des Télécommunications et de l'Agence nationale de la sécurité informatique, ainsi que des entreprises de télécommunications.

> S'APPUYANT SUR LES RECOMMANDATIONS DE LA RÉCENTE ÉTUDE DE L'ORGANISATION MONDIALE DE LA SANTÉ SUR L'EFFICACITÉ ET L'IMPACT DES INTERVENTIONS CIBLANT LA VIOLENCE SEXUELLE, IL Y A L'EXEMPLE D'INTERVENTIONS FONDÉES SUR LE CURRICULUM DANS LES PAYS À REVENU FAIBLE ET INTERMÉDIAIRE QUI CIBLENT LES RISQUES SEXUELS PSYCHOSOCIAUX ET TRAITENT LES RISQUES MULTIPLES ET FACTEURS DE PROTECTION AFFECTANT LES COMPORTEMENTS SEXUELS (TELS QUE LES CONNAISSANCES, LES RISQUES PERÇUS, LES VALEURS, LES ATTITUDES, LES NORMES PERÇUES ET L'EFFICACITÉ AUTONOME). IL EST DÉMONTRÉ QUE CES RÉSULTATS ONT TOUJOURS DES RÉSULTATS POSITIFS SUR LES ENFANTS ET PEUVENT ÊTRE ADAPTÉS POUR INCLURE DES MODULES, DES COMPOSANTS ET DES EXEMPLES DE VIOLENCE EN LIGNE.

2.8. Renforcer l'offre de soutien psychosocial pour les enfants

Compte tenu du manque de ressources financières de l'État, cela peut être réalisé en assurant une meilleure affectation des psychologues et pédopsychiatres affiliés au gouvernement existant, et en réactivant des bureaux d'écoute et de conseil (BEC) et les cellules d'écoute et de conseil (CEC).

Compte tenu des contraintes de capacité et du nombre limité de travailleurs sociaux de première ligne du gouvernement et de travailleurs de la protection de l'enfance, il peut être important de tirer parti de la portée, de la capacité et de la volonté des organisations de la société civile pour fournir des services de qualité aux enfants. Bien qu'aucune organisation se concentrant spécifiquement sur les risques en ligne ou les expériences en ligne des enfants n'ait été identifiée au cours de cette étude, plusieurs organisations fournissant des services de prévention et d'intervention plus larges aux enfants ont exprimé leur volonté d'aider le gouvernement à fournir des services psychosociaux et de protection. De telles organisations pourraient fournir des atouts précieux en veillant à ce que davantage de services atteignent plus d'enfants. Cela doit être entrepris à travers des accords de partenariat qui obligent les acteurs de la société civile à maintenir la confidentialité et l'anonymat des enfants

3. Recommandations institutionnelles

Le modèle de réponse nationale est explicite quant à la nécessité d'une collaboration intersectorielle et de mécanismes appropriés dans toute stratégie efficace de protection de l'enfance. Il en va de même pour tous les aspects de la protection en ligne des enfants. Les recommandations suivantes se rapportent à des considérations institutionnelles.

3.1. Assurer la coordination intergouvernementale sur la protection en ligne des enfants

La protection des enfants en ligne devrait être intégrée dans tous les ministères impliqués dans des activités avec ou fournissant des services aux enfants, y compris l'éducation. Dans le cas de l'éducation, c'est d'autant plus vrai que le ministère pilote l'utilisation des tablettes et des TIC dans les écoles. En Jordanie, le ministère de l'Éducation a introduit un programme de formation en ligne sur la protection pour tous les enseignants dans le contexte de la COVID, alors que l'éducation se déplaçait en ligne.[49] Alors que ce processus en est à ses débuts en Tunisie, l'introduction de mesures de protection en ligne et le renforcement des capacités des enseignants dès le départ deviendront de plus en plus importants. Les directives mondiales sur la protection en ligne des enfants et l'utilisation de l'EdTech fournies par l'UNICEF peuvent constituer un point de départ précieux pour ce processus.[50]

Le comité de pilotage créé aux fins de ce projet constitue un excellent point de départ pour un mécanisme de coordination chargé de superviser la mise en œuvre de ces recommandations, ainsi que de soutenir et de piloter le PAN. Cependant, il est important qu'un groupe de travail ou un organe de coordination sur la protection en ligne des enfants ait le poids politique et l'autorité nécessaires pour conduire le PAN, étant donné que le PAN nécessitera un engagement (y compris budgétaire) de la part de chacun des ministères de tutelle impliqués dans une réponse globale à la violence en ligne. Il est également proposé qu'au lieu de se présenter comme une entité distincte, le groupe de travail ou l'organe de coordination soit une sous-structure d'un groupe de travail interministériel ou départemental plus large sur la protection de l'enfance. Enfin, il sera important que d'autres acteurs, y compris la société civile, l'industrie et les organismes de recherche soient représentés dans cette structure.

Exemples régionaux d'intégration de la protection en ligne dans le système de protection de l'enfance

Des exemples d'intégration de la protection en ligne des enfants dans le système formel de protection de l'enfance peuvent être trouvés au Maroc et en Égypte. Au Maroc, le gouvernement s'est engagé dans un processus détaillé d'intégration des systèmes d'intervention en matière de protection de l'enfance qui comprenait les ministères de l'Education, de la Santé, de la Justice et de la Jeunesse et des Sports, entre autres, et a identifié où une formation spécialisée sur la violence en ligne était nécessaire. Ce processus, bien qu'il soit principalement axé sur la prévention et l'intervention, offre également l'avantage potentiel de promouvoir la cohérence entre ces ministères dans la diffusion de messages communs.

49 https://www.unicef.org/jordan/reports/online-safeguarding
50 United Nations Children's Fund, 'Child Protection in Digital Education: Policy Brief', UNICEF, New York, December 2022.

3.2. Intégrer la protection en ligne dans le mécanisme formel de protection de l'enfance

Le renforcement du système de protection de l'enfance et la mise en place d'un système intégré de gestion des cas est déjà en cours en Tunisie et l'intégration des risques en ligne devrait être intégrée dans ce processus. Cela peut constituer la base du renforcement du système de protection pour assurer la préparation et la capacité à traiter de manière adéquate les cas de violence sexuelle et d'autres formes de violence en ligne qui nécessitent une intervention ou une gestion formelle de la protection de l'enfance.

Compte tenu de la complexité des comportements et des risques liés à des activités telles que le sextage (sexting) et les images auto-générées, il est important que le système de protection de l'enfance et le système judiciaire répondent aux besoins des enfants, ainsi qu'aux circonstances et protections particulières dont ils ont besoin. Une façon de gérer cela est de garantir des tribunaux adaptés aux enfants et des centres « à guichet unique », qui protègent l'anonymat et la confidentialité des enfants, minimisent les nouveaux traumatismes et encouragent le signalement dans un environnement sûr où les enfants peuvent être garantis autant que possible aucune stigmatisation.

Les juges pour enfants en Tunisie ont déjà reçu une formation considérable sur la justice adaptée aux enfants. Cela fournit un point d'entrée important pour améliorer la réponse judiciaire à l'extorsion en ligne et à d'autres formes de problèmes criminels et procéduraux potentiels concernant les enfants dans l'espace numérique et la protection de l'enfance, en particulier dans le contexte des centres à guichet unique.

En Tunisie, le partenariat du Conseil de l'Europe avec le ministère de la Justice pour la mise en place des guichets uniques Barnahus peut constituer un premier point d'entrée pour former et soutenir le service de protection et d'intervention judiciaire sur la protection en ligne. Bien que le modèle n'ait pas été évalué spécifiquement pour ses résultats positifs sur les enfants signalant des abus sexuels en ligne ou qui sont impliqués dans des affaires d'extorsion en ligne, le modèle a été identifié comme une pratique prometteuse pour améliorer la prestation de services et la justice pour les enfants qui sont soit victime ou auteur. Se concentrer sur un soutien ciblé aux fonctionnaires de la justice, des juges, des procureurs, de la police et des agents de protection de l'enfance, au sein de ces sites sélectionnés facilitera également la collecte de données fiables sur les cas, et la manière dont ceux-ci sont gérés au sein du système intégré de protection de l'enfance, et en fin de compte, fournira un point de départ utile pour une évaluation de telles interventions spécifiquement sur les résultats de sécurité en ligne.

Liste des annexes

- **Annexe 1:** Revue de la Littérature
- **Annexe 2:** Cartographie du cadre juridique et institutionnel pour la protection de l'enfant en ligne en Tunisie
- **Annexe 3:** Indicateurs pour la sélection des sites de recherche
- **Annexe 4:** Protocole de recherche
- **Annexe 5:** Liste des entretiens avec les principales parties prenantes
- **Annexe 6:** Liste des réponses qualitatives des enfants au questionnaire d'enquête anonyme

Appendix 1 : Revue de la littérature

I. Introduction

La présente revue de la littérature a été préparée dans le cadre d'une étude de recherche qui sera utilisée pour élaborer un plan d'action national pour la prévention de la violence en ligne contre les enfants en Tunisie. Cette recherche est menée par le Centre de Justice et Prévention de la Criminalité et Resolve Consulting pour l'UNICEF Tunisie et le ministère de la Femme, de la Famille, de l'Enfance et des Seniors - MFFES).

1. Approche analytique

Cette revue de la littérature s'appuie sur la littérature scientifique évaluée par des pairs, les données administratives générées par le gouvernement tunisien ou par des organismes et institutions internationaux/régionaux, et des rapports d'experts du secteur. La législation et les politiques pertinentes dans divers secteurs, notamment la sécurité, la justice, la protection sociale, l'éducation, les affaires religieuses et les technologies de l'information, sont également examinées. Cet examen met un accent particulier sur l'identification des politiques et des mesures gouvernementales existantes pour l'incorporation de tous les aspects liés à l'identification, la prévention et la réponse à la violence en ligne, et le degré de leur alignement avec les orientations et les cadres mondiaux (y compris le MNR et INSPIRE, comme ainsi que des conseils terminologiques et un cadrage des droits de l'enfant tel qu'énoncé dans l'OG.25), en tenant compte du contexte tunisien et régional. Cela vise à identifier les lacunes, ainsi que le besoin potentiel d'harmonisation entre la législation et la politique.

2. Limites

Il s'agit d'une revue de la littérature qui identifie de manière sélective les textes clés et une large couverture des études sur la protection en ligne de l'enfant, la mise en œuvre d'une « approche des droits de l'enfant », les liens entre la violence en ligne et hors ligne, la façon dont les risques en ligne peuvent conduire à la fois en ligne et les préjudices hors ligne et le maintien des droits des enfants en équilibrant les risques et les opportunités associés à la privation des enfants de l'accès à la technologie.

Cependant, comme cette recherche n'est pas aussi complète qu'une revue systématique de la littérature, il est plausible que toutes les meilleures pratiques ou études internationales n'aient pas été incluses. En outre, la littérature examinée contient un préjugé favorable à l'égard des études universitaires en anglais, mais les rapports, les lois et les stratégies en français et en arabe des ministères et organismes de recherche tunisiens sont également analysés dans l'annexe 2. Le travail de Sonia Livingstone est largement présent dans cette revue parce qu'elle est une leader dans le domaine qui a apporté des contributions théoriques et empiriques exceptionnelles.

II. Les enfants en ligne en Tunisie

La population tunisienne s'élève à 11,9 millions d'habitants, dont 20,3 % (environ 2 433 970) sont âgés de 5 à 17 ans. La Tunisie a un taux de pénétration d'internet de 66,7%. Sur les 8,15 millions d'utilisateurs de médias sociaux, 7,1 millions utilisent Facebook, le troisième site Web le plus visité, après Google et YouTube.[1] Nonobstant les disparités régionales, l'utilisation d'internet, et en particulier des réseaux sociaux, est prépondérante chez les enfants et adolescents tunisiens. Selon une enquête de 2017 ,[2] les adolescents tunisiens âgés de 15 à 17 ans utilisent Internet 3 à 5 jours par semaine en moyenne, tandis que 43,9 % utilisent quotidiennement les réseaux sociaux.

Malgré la hausse documentée de la violence en ligne contre les enfants à l'échelle mondiale, un rapport de l'UNICEF a souligné le manque de données systémiques spécifiques sur la violence en ligne affectant les enfants en Tunisie.[3] Cela met en exergue l'absence d'une stratégie et d'un mécanisme clairs pour identifier et documenter les diverses formes de violence et de menaces en ligne ciblant les enfants. À son tour, cela entrave toute tentative de lutter efficacement contre ce phénomène d'une manière qui tient compte simultanément du droit des enfants à accéder à Internet et à en bénéficier.

La pandémie de COVID-19 a mis en évidence l'importance de la technologie numérique dans la vie des enfants. Les périodes de confinement ont forcé les enfants à passer plus de temps en ligne et ont considérablement réduit leurs possibilités de jouer à l'extérieur, de rencontrer des amis et de la famille en dehors de leur famille immédiate ou de se livrer à des activités physiques sociales. L'interaction avec les amis et les pairs à l'école a été réduite de la même manière, la scolarité se déplaçant, dans une large mesure, vers l'espace en ligne.

La pandémie a également mis en évidence les inégalités existantes dans l'accès à la technologie et au haut débit, en particulier en dehors des centres urbains. Cela a un impact à la fois sur l'accès à la technologie et à l'infrastructure technologique, mais aussi sur la littératie numérique des enfants et des jeunes en ligne.

En Tunisie, les inégalités socio-économiques régionales historiques ont été aggravées par un « fossé numérique » défavorisant les enfants marginalisés des régions intérieures pauvres. Les enfants représentent 29% de la population tunisienne, ils représentent 40% des pauvres du pays. En outre, les enfants vivant dans les régions rurales de l'intérieur courent un risque accru de vivre dans la pauvreté ou l'extrême pauvreté. Cette précarité a été encore exacerbée par le Covid-19, les taux de pauvreté étant passés de 15,2 % à 19,1 % et l'extrême pauvreté de 2,9 % à 3,3 %.[4]

Ces conditions conduisent à une précarité multidimensionnelle des enfants et à l'enracinement des disparités régionales. Par exemple, en raison des inégalités d'accès aux soins de santé, les régions rurales de l'intérieur enregistrent des taux de mortalité infantile plus élevés (19/1000 contre 11/1000 dans les régions urbaines en 2018)[5] .

1 Kemp, Simon (2021) Numerqiue 2021 : Tunisie. DataReportal. https://datareportal.com/reports/digital-2021-tunisia#:~:text=There%20were%207.92%20million%20internet,at%2066.7%25%20in%20January%202021.
2 UNICEF Tunisie (2020) Analyse de la situation des enfants en Tunisie. p. 128 https://www.unicef.org/tunisia/rapports/analyse-de-la-situation-des-enfants-en-tunisie-2020
3 Idem.
4 Ministère de la Femme, de la Famille et des Séniors (2021) Projet de la politique publique intégrée de la prévention et de protection des enfants. p. 4 http://www.femmes.gov.tn/wp-content/uploads/2017/07/Resum%C3%A9-excutif.pdf
5 Idem, p. 4

L'inégalité d'accès à des infrastructures et à des services d'éducation adéquats a fait que les régions de l'intérieur souffrent de taux plus élevés d'abandon scolaire au primaire et au secondaire et de taux plus élevés d'échec au baccalauréat. Les taux de décrochage scolaire des enfants des régions pauvres de l'intérieur sont 2,5 fois plus élevés que la moyenne. En 2021, les régions côtières les plus aisées de Sousse et Monastir ont enregistré des taux de réussite au baccalauréat de 61% et 62,5% respectivement, tandis que les taux dans les régions intérieures de Tataouine (sud-est) et Jendouba (nord-ouest) étaient de 38,6% et 35,7% respectivement.[6]

L'inégalité d'accès à Internet et aux outils informatiques a renforcé les inégalités socio-économiques régionales existantes pendant la pandémie. Par exemple, "les enfants (...) dotés en équipement approprié (ordinateur, imprimante, et accès à l'internet permettant un enseignement virtuel) seront en meilleure prédisposition pour combler les déficits d'enseignement occasionnés par la fermeture des écoles et lycées pendant plusieurs mois."[7]

Ces inégalités génèrent et exacerbent à leur tour d'autres inégalités qui peuvent directement exposer les enfants à un plus grand risque de divers types de violence. Les enfants ayant des niveaux inférieurs de littéraire numérique peuvent être désavantagés lorsque l'éducation est en ligne, ce qui entraîne des résultats scolaires inferieurs à leurs pairs (en supposant qu'ils peuvent même se connecter), lui-même un facteur de risque de violence. Ces enfants peuvent également être plus vulnérables à certains types de violence qui se produisent à la fois en ligne et hors ligne, comme l'exploitation sexuelle des enfants en ligne.

III. Risques et préjudices en ligne : considérations clés

Malgré quelques problèmes de définition, il existe un consensus général dans la littérature et les politiques sur le fait que les risques en ligne peuvent être opérationnalisés en trois catégories : contenu, contact et conduite .[8] En outre, sur la base des développements récents et d'un nombre croissant de preuves sur les risques commerciaux et de confidentialité auxquels sont confrontés les enfants en ligne, une quatrième catégorie peut être ajoutée, à savoir les risques contractuels :

- Les risques liés au contenu incluent ceux où les enfants interagissent avec ou sont exposés à un contenu potentiellement préjudiciable;
- Les risques de contact décrivent tous les cas où l'enfant subit ou est exposé à un contact adulte potentiellement dangereux;
- Les risques de comportement font référence à des scénarios dans lesquels l'enfant lui-même participe ou est victime d'un comportement potentiellement préjudiciable de ses pairs ;
- Les risques contractuels concernent les risques auxquels sont exposés les enfants lorsqu'ils sont impliqués dans des risques contractuels potentiellement préjudiciables ou peuvent être exploités par eux.

6 BAC Tunisie (2021) Taux de réussite par section et par région. https://www.bac.org.tn/bac-tunisie-2021-taux-de-reussite-par-section-et-par-region/#:~:text=On%20retrouve%20par%20la%20suite,2%20avec%2055%2C31%25.
7 Mahjoub, Azzam (2020) Pandemie Covid 19 en Tunisie : Les inégalités, les vulnérabilités à la pauvreté, et au chômage. Forum Tunisien pour les Droits Economique et Sociaux. p.9 http://ftdes.net/rapports/COVID-AZ19.pdf
8 Livingstone, Mascheroni & Staksrud, (2015); Staksrud & Livingstone, (2009)

CORE	Contenu	Contact	Conduite	Contract
	Enfants interagissent avec ou sont exposés à un contenu potentiellement préjudiciable	Où l'enfant subit ou est exposé à un contact adulte potentiellement dangereux	L'enfant lui-même participe ou est victime d'un comportement potentiellement préjudiciable de ses pairs	Les enfants lorsqu'ils sont impliqués dans des risques contractuels potentiellement préjudiciables ou peuvent être exploités par eux.
Agressif	Violent, sanglant, graphique, raciste, odieux, ou information et communication extrémiste	Harcèlement, comportement haineux, surveillance indésirable ou excessive	Intimidation, communication haineuse ou hostile ou activité des pairs . Exemple: insultes en ligne, exclusion, humiliation	Vol d'identité, fraude, hameçonnage, escroqueries, piratage, chantage, risque de sécurité.
Sexuel	Pornographie, (nocif ou illégal), sexualisation de la culture, normes d'image corporelle oppressives	Harcèlement sexuel, sollicitation sexuelle, sextor-sion, génération et partage de maté-riels d'abus sexuel d'enfant	Harcèlement sexuel, message-rie sexuelle non consensuelle, pressions sexuelles défavorables	Traite à des fins d'exploitation sexuelle, streaming (payé pour) d'abus sexuel d'enfant
Valeurs	Désinformation, marketing inapproprié à l'âge ou contenu généré par l'utilisateur	Conviction idéologique ou manipulation, radicalisation et recrutement extrémiste	Communautés d'utilisateurs potentiellement nuisibles, par exemple l'automutilation, anti-vaccin, pressions défavorables des pairs	Jeux d'argent, filtrer les bulles, mi-cro-ciblage, motifs sombres façonnant la persuasion ou l'achat
Transversal	Violation de la vie privée (interpersonnelle, institutionnelle, commerciale) Risques pour la santé physique et mentale (exemple : mode de vie sédentaire, utili-sation abusive de l'écran, isolement, anxiété) Inégalités et discriminations (exclusion, exploitation de la vulnérabilité, biais algo-rithmique, analyses prédictives)			

Le tableau ci-dessous présente la classification CO: RE des principaux risques en ligne affectant les enfants, selon les quatre catégories susmentionnées.[9]

Les risques en ligne peuvent inclure plusieurs expériences différentes, allant des atteintes à la vie privée et de l'intimidation à la rencontre de contenus racistes, haineux, violents ou pornographiques, chacune pouvant être classée selon la typologie présentée ci-dessous.[10]

L'interconnexion entre les risques auxquels les enfants sont confrontés en ligne et les dommages qu'ils peuvent encourir en ligne ou hors ligne est établie dans la littérature. Cependant, la littérature indique également que les risques en ligne ne conduisent pas intrinsèquement à des préjudices en ligne ou hors ligne. Bien que ces risques soient souvent considérés comme dangereux, le risque n'est qu'une indication du danger potentiel d'Internet. Le préjudice résultant du risque est un indicateur plus précis de ce qui rend Internet dangereux. [11]

Un risque qui différencie souvent l'abus en ligne de l'abus hors ligne est lorsqu'un enfant rencontre un étranger en personne/hors ligne qu'il a rencontré pour la première fois en ligne. Les risques liés à cette gamme vont de l'agression sexuelle et de l'enlèvement au matériel d'abus sexuel d'enfants. De plus, il existe un risque que la sollicitation sexuelle ait eu lieu avant la rencontre. Pourtant, le fait de rencontrer quelqu'un hors ligne, dans la vraie vie, alors que le contact a initialement été établi en ligne, est souvent l'un des attraits du chat ou de l'engagement en ligne. Internet offre la possibilité aux enfants, qu'ils soient dans des communautés traditionnelles ou intégrées ou dans des milieux marginalisés ou isolés, de s'engager au-delà de leur cercle immédiat ou de leur cadre de référence[12]. Les données de l'étude Global Kids Online[13] , une recherche menée dans quatre pays du Sud, montrent que 30 % des enfants ont rencontré en personne quelqu'un qu'ils ont rencontré pour la première fois en ligne. Bien que ces enfants aient été « à risque » en rencontrant un étranger, l'étude n'a pas saisi combien d'entre eux ont été victimes d'un type de préjudice. Peu de preuves sont disponibles sur la nature et l'étendue des expériences de préjudice en ligne des enfants. En effet, très peu d'études ont tenté de saisir la prévalence des dommages. Après tout, il est difficile d'opérationnaliser et de capturer éthiquement des données sur le degré auquel les enfants sont bouleversés par ce qu'ils rencontrent en ligne[14] . D'autres ont utilisé des listes de contrôle de la santé mentale pour saisir les dommages psychologiques pouvant résulter d'expériences en ligne. [15]

Il existe quelques exceptions aux termes généraux dans lesquels le préjudice est généralement analysé. Celles-ci ont eu tendance à se concentrer très spécifiquement sur les méfaits qui pourraient être associés au harcèlement sexuel, à la pornographie et à la cyberintimidation.[16]

La mesure dans laquelle le risque se traduit par un préjudice, et en fait l'étendue des préjudices eux-mêmes, est encore compliquée par le fait que les risques et les préjudices traversent le monde en ligne et hors ligne.[17]

9 Sonia Livingstone and Mariya Stoilova, "The 4Cs: Classifying Online Risk to Children," CO:RE Short Report Series on Key Topics (Hamburg, Germany: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI), 2021), 12, https://doi.org/10.21241/ssoar.71817.
10 Staksrud & Livingstone, (2009)
11 Staksrud & Livingstone, 2009; Slavtcheva- Petkova (date) Nash & Bulger, 2015).
12 CJCP, 2012; Boyd, 2014
13 Global Kids Online (2017) FULL reference required.
14 Livingstone & Helsper, (2010); Slavtcheva- Petkova, Nash & Bulger (2015)
15 David Smahel et al. (2020) Survey Results from 19 Countries". EU Kids Online. Doi: 10.21953/lse.47fdeqj01ofo.
16 Henry, N., & Powell, A. (2018). Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research. Trauma, Violence, & Abuse, 19(2), 195–208.
17 Livingstone (2013)

Livingstone soutient que «pour les risques les plus graves (tels que la sollicitation sexuelle, ou une exposition prolongée à la pornographie extrême, ou une telle intimidation soutenue qu'un enfant est poussé à l'automutilation), on suppose souvent que, bien que le risque soit rencontré en ligne, le préjudice aura lieu hors ligne ». Cela permet aux agences de protection de l'enfance et aux services d'intervention de répondre au préjudice qui en résulte comme ils le feraient pour tout autre cas d'abus. Cependant, à mesure que le fossé entre la vie en ligne et hors ligne, en plus des facteurs de risques et de préjudices en ligne et hors ligne, s'estompe, les agents d'intervention sont de plus en plus tenus d'examiner comment les services englobent à la fois les espaces en ligne et hors ligne.

L'intimidation fournit un contexte utile pour examiner les interventions efficaces en ligne et hors ligne. La plupart des travaux sur l'exploration de la relation entre le risque en ligne et hors ligne se sont concentrés sur l'intimidation et la cyberintimidation, et sur la relation entre l'intimidateur et la victime, à la fois en ligne et hors ligne.

Grâce à cet ensemble de travaux, la relation entre le risque d'être victime d'intimidation, physiquement ou émotionnellement hors ligne - souvent appelée intimidation dans la cour d'école - et la probabilité d'être victime d'intimidation en ligne a été établie.[18]

La relation cyclique entre le harcèlement en ligne et hors ligne reste claire. L'étude EU Kids Online a montré que 60 % des enfants qui intimident eux-mêmes en ligne ont eux-mêmes été victimes d'intimidation, en ligne ou hors ligne (l'espace dans lequel cela se produit n'étant pas significatif), tandis que 40 % de ceux qui intimident en ligne ont eux-mêmes été victimes d'intimidation en ligne.[19] Il est important de noter que cela reflète également le même risque que ceux qui ont été victimes d'intimidation en ligne deviennent eux-mêmes des intimidateurs en ligne, comme cela a été reconnu depuis longtemps dans l'espace hors ligne. [20] De même, dans l'étude de la Fondation Optimus sur la maltraitance, la violence et la négligence des enfants en Afrique du Sud, un une forte relation s'est produite entre l'intimidation en ligne et hors ligne.[21] Ceux qui ont été victimes d'intimidation étaient susceptibles d'avoir vécu cela en ligne et hors ligne, ainsi que l'expérience de transition entre en ligne et hors ligne. [22]

Des études se sont également penchées sur la mesure dans laquelle le risque en ligne émule ou s'étend du risque hors ligne et la mesure dans laquelle le risque hors ligne prédit le risque en ligne. Alors que la comorbidité est de plus en plus documentée, les voies causales sont moins comprises. Les enfants qui signalent plus de risques hors ligne sont plus susceptibles de signaler plus de risques en ligne, ainsi que d'être plus susceptibles de signaler des préjudices résultant de la rencontre de ces risques en ligne.[23] de violence, y compris la violence sexuelle, l'exposition à la violence et la maltraitance des enfants.[24]

Bien qu'il se soit avéré impossible de déterminer la causalité ou les voies (c'est-à-dire les voies d'une forme de violence en ligne ou hors ligne à une autre, ou quelle violence est antérieure à l'autre), les recherches existantes identifient la forte association entre la violence en ligne et d'autres formes de violence hors ligne pouvant provenir de plusieurs facteurs. La relation entre la vulnérabilité et l'expérience de multiples formes de violence (poly victimisation) et la violence dans

18 Wolak 2007
19 Patchin and Hinduja, 2006; Smith et al, 2006; and Jang et al, 2013
20 Menesini, (2017).
21 Optimus Study (2016) Sexual abuse of children and adolescents in South Africa: Forms, extent and circumstances. UBS Optimus Foundation https://www.ubs.com/global/de/ubs-society/philanthropy/blog/2018/child-sexual-abuse.html
22 Burton et al, (2017).
23 EU and Global Kids Online studies -
24 Burton et al, forthcoming

différentes sphères (foyer, école, communauté) est bien documentée .[25] Les enfants victimes de poly victimisation sont plus susceptibles de subir un traumatisme que ceux qui subissent un seul incident ou une seule forme de violence.[26]

Les enfants exposés à la violence ou victimes hors ligne (y compris la victimisation sexuelle) peuvent utiliser l'espace en ligne pour rechercher du soutien et de la compagnie, ou établir des relations plus sûres que les relations hors ligne, de la même manière que les enfants socialement isolés hors ligne peuvent nouer des relations plus solides ou trouver des espaces sûrs en ligne. Cependant, malgré la conclusion positive selon laquelle les enfants qui souffrent hors ligne peuvent trouver du soutien et du réconfort en ligne, d'autres études montrent que les expériences de violence hors ligne peuvent également entraîner la dépression, l'anxiété et le retrait social, et il a été démontré que d'autres résultats psychologiques liés aux traumatismes augmentent le risque à la fois pour la cyberintimidation et les abus sexuels en ligne tels que la sollicitation sexuelle.[27]

Il existe également des caractéristiques communes aux différentes formes de violence hors ligne, notamment physique et sexuelle, qui sont communes aux caractéristiques de la violence en ligne. Par exemple, la violence interpersonnelle, la violence sexuelle et le harcèlement sont le plus souvent commis par des personnes connues de l'enfant, une caractéristique partagée par les enfants victimes de harcèlement en ligne.

Une étude sur le harcèlement en ligne aux États-Unis démontre que les adultes victimes de violence conjugale (VPI) sont plus susceptibles d'être victimes de harcèlement en ligne que ceux qui n'ont pas subi de violence conjugale.[28] Il est donc plausible que les expériences des enfants victimes de formes de violence sexuelle ou domestique ne soient pas différentes.

Malgré des études qui montrent comment les actions en ligne peuvent entraîner des conséquences hors ligne et vice versa, d'autres publications établissent comment la violence imprègne la fracture en ligne et hors ligne et est fondamentalement interconnectée. Cette intersection entre la violence en ligne et hors ligne est évidente dans la manière dont la violence est vécue, la nature de la violence et son impact sur les victimes. Kardefelt-Winther et Maternowska présentent trois scénarios pour illustrer ce point.

- « #1 : Un enfant est abusé sexuellement à la maison et l'acte est photographié. Les images sont vendues en ligne et largement partagées. S'agit-il d'un cas de violence sexuelle en ligne ou de violence sexuelle à la maison ?
- #2 : Un enfant reçoit un message blessant et menaçant sur un site de réseautage social. L'enfant arrive à l'école en se sentant intimidé par ses camarades de classe. Cela constitue-t-il du cyber-harcèlement, de la violence entre pairs ou de la violence en milieu scolaire ? »
- #3 : Un enfant envoie des images explicites à un partenaire, qui les partage avec ses camarades de classe. Les images se sont propagées sur les réseaux sociaux et l'enfant est victime d'intimidation. Finalement, l'enfant se suicide. Cela constitue-t-il de la violence en ligne, des abus sexuels ou de la violence en milieu scolaire ? » [29]

25 Finkelhor et al. (2015), Leoschut & Kafaar, (2017)
26 Samms-Vaughan and Lambert (2017)
27 Merrill et al, (2016); Whittle et al, (2013).
28 Ybarra et al, (2017)
29 Kardefelt-Winther, D., Maternowska, C. Addressing violence against children online and offline. Nature Human Behaviour. 4, 227–230 (2020). https://doi.org/10.1038/s41562-019-0791-3

Cette section démontre que la violence en ligne se présente sous différentes formes et que la relation entre la violence en ligne et hors ligne est souvent mutuellement constitutive. Bien que l'exposition aux risques puisse entraîner des préjudices, les risques en ligne ne sont toutefois pas intrinsèquement liés aux préjudices en ligne ou hors ligne. Par conséquent, comme l'aborde la section suivante, il est essentiel de s'assurer que les enfants sont conscients des risques et que leurs droits d'accès à Internet ne sont pas restreints.

IV. Mettre fin à la violence contre les enfants tout en protégeant leurs droits

L'accès à Internet est un droit de l'enfant. La privation d'accès à internet, au 21e siècle, risque de freiner leur développement. Cependant, la distinction floue entre en ligne et hors ligne signifie qu'il est «plus complexe que jamais de déterminer la meilleure façon d'assurer la sécurité des enfants» et qu'il est «difficile de faire progresser la prévention et la réponse fondées sur des données probantes». [30] Pour aborder ce défi complexe, cette section passe en revue la littérature sur la vulnérabilité des enfants à la violence en ligne en plus du droit et du besoin de développement pour les enfants d'avoir accès à Internet.

1. Vulnérabilité des enfants à la violence en ligne

Pour faire face aux risques en ligne, il faut comprendre si certains facteurs ou conditions augmentent le risque et rendent ainsi les enfants plus vulnérables à la violence en ligne. Cependant, il s'agit d'une tâche exceptionnellement difficile lorsque la littérature identifie que l'âge, le sexe, l'orientation sexuelle, la capacité cognitive, le comportement, l'emplacement et la région du monde de l'enfant affectent l'analyse. De plus, la littérature suggère que les liens entre les réponses en ligne et hors ligne devraient être maintenus.

Premièrement, «il n'y a pas suffisamment de preuves pour fournir une indication sans ambiguïté quant à savoir si les risques associés aux activités en ligne sont les mêmes ou ont les mêmes implications pour les enfants dans différentes régions du monde». [31] En plus des différents risques dans différents contextes, le risque n'est pas statique, et les enfants ne le vivent pas seuls tout au long de leur enfance. Un examen des supports pédagogiques pour la prévention de l'exploitation et des abus sexuels d'enfants dans des contextes en ligne et hors ligne permet de comprendre comment les expériences de risque changent au fil du temps. Il démontre que les types et la fréquence des risques auxquels les enfants sont exposés, en plus de la façon dont les enfants sont susceptibles de réagir, changent tout au long de leur enfance. «L'utilisation d'Internet par les enfants, ainsi que leur comportement et leurs vulnérabilités en ligne diffèrent en fonction de leur âge». [32] Ainsi, la vulnérabilité des enfants au risque évolue tout au long de leur enfance.

30 Kardefelt-Winther & Maternowska (2020)
31 Innocenti Research Centre (2011) Child safety online: Global challenges and strategies. UNICEF p.6
32 Innocenti Research Centre (2011) Child safety online: Global challenges and strategies. UNICEF p. vii

Il se déplace également à travers différents domaines de la vie quotidienne - les maisons, les écoles, les communautés - et l'intersection que l'espace en ligne fournit à travers ces domaines physiques et sociaux. Par exemple, les enfants plus âgés sont plus susceptibles d'être exposés à des risques en ligne que les enfants plus jeunes.[33]

Les enfants peuvent également accroître leur vulnérabilité en adoptant des comportements à risque. Ybarra et al (2006) ont constaté que « les jeunes qui adoptent des comportements à risque lorsqu'ils sont en ligne » deviennent vulnérables aux mêmes risques. Ainsi, ceux qui intimident ou harcèlent en ligne sont plus susceptibles d'être également victimes d'intimidation ou de harcèlement. Cette étude a également démontré comment la distinction entre en ligne et hors ligne peut s'estomper, car «une cible de harcèlement sur Internet sur 4 signale un contact hors ligne agressif de la part de l'harceleur, comme un appel téléphonique ou une visite à son domicile». [34]

Les résultats sont mitigés en termes de sexe et de risque en ligne. Certaines études montrent que les garçons et les filles sont également susceptibles de subir certaines formes de risque liées au harcèlement en ligne.[35] D'autres montrent que les filles sont plus susceptibles d'être victimes de harcèlement sexuel tandis que les garçons sont plus susceptibles d'être exposés à la pornographie et aux images graphiques.[36] Alors que les garçons peuvent être plus susceptibles de rencontrer des risques en ligne, les filles sont plus susceptibles de déclarer être en détresse à la suite de ces risques encourus.[37]

Alors que l'exposition et l'expérience des risques en ligne changent tout au long de l'enfance, il est également important de s'engager avec les changements potentiels de la vulnérabilité. Une optique de vulnérabilités pour aborder les risques et les préjudices en ligne offre un cadre utile pour identifier où les enfants pourraient être exposés à un risque plus élevé ou anticiper où le risque pourrait se traduire par des préjudices tangibles et mesurables. Si, par exemple, les enfants socialement isolés semblent subir des niveaux plus élevés de cyberintimidation, les interventions éducatives peuvent être ciblées sur ces enfants et la capacité des éducateurs, des parents et des autres soignants à identifier et à intervenir tôt peut être développée.

L'un des dangers de cette situation est que la vulnérabilité aux risques en ligne est perçue comme une vulnérabilité en ligne, plutôt qu'une vulnérabilité dans tous les domaines, à la fois en ligne et hors ligne. Un exemple serait dans les écoles ou les environnements où la cyberintimidation a été identifiée comme une préoccupation, et donc les interventions contre la cyberintimidation sont proposées indépendamment des interventions plus larges en matière d'intimidation, de normes sociales ou de changement de comportement.

Malgré ce danger, une compréhension des vulnérabilités en ligne et hors ligne est essentielle pour cibler efficacement les mesures - politiques et programmes - qui peuvent mieux équiper ceux qui sont les plus à risque, et les moments ou les endroits de leur vie où ces vulnérabilités sont les plus grandes. La nécessité de mieux comprendre comment les vulnérabilités se recoupent avec les risques en ligne et les TIC en général est de plus en plus reconnue.[38]

33 Wells et al, 2014; Phyfer et al 2016
34 Ybarra et al, 2006: 1174.
35 Ybarra et al 2006
36 Ybarra et al 2006
37 Phyfer et al, 2016; Livingstone and Hadden, 2009; De Graaf and Vanweesenbeek, (2006).
38 Livingstone et al, 2017; Wells et al 2014; Byrne & Burton, 2017; Mitchell et al, 2014,

Bien qu'elle ne soit pas exhaustive, une discussion émergente sur les vulnérabilités fondées sur l'identité sexuelle et les minorités sexuelles. Il est de plus en plus évident que les enfants issus de groupes minoritaires, y compris les groupes LGBT, souffrant de handicaps physiques ou mentaux, ou de minorités ethniques sont les plus à risque d'être victimes d'intimidation.[39] Dans une étude sur des enfants suédois, la bi- ou l'homosexualité s'est avérée être le facteur le plus important pour prédire la sollicitation sexuelle en ligne.[40] Parmi les 13 à 18 ans, ceux qui s'identifiaient comme LGBT étaient disproportionnellement exposés au risque d'être victimes de harcèlement sexuel en particulier en ligne.[41] La même étude a également montré le transect entre en ligne et hors ligne, le harcèlement sexuel étant le plus souvent vécu hors ligne, suivi du harcèlement en ligne.[42] Le risque accru que les enfants des minorités sexuelles soient victimes de victimisation en ligne semble suivre la même vulnérabilité de la violence hors ligne. Une étude de 2011 aux États-Unis montre des résultats similaires concernant la cyberintimidation des groupes LGBT, avec près du double du nombre d'enfants s'identifiant aux LGBT que d'enfants hétérosexuels déclarant être victimes de cyberintimidation, un résultat similaire à ceux qui ont été victimes d'intimidation hors ligne.[43] De même, une étude de 2013 aux États-Unis montre que les jeunes LGBT étaient trois fois plus susceptibles que les jeunes non LGBT d'être victimes d'intimidation ou de harcèlement en ligne. [44]

Alors qu'Internet offre un espace sûr d'interaction sociale pour ceux qui peuvent être socialement isolés en raison, par exemple, de leur identité sexuelle, il en va de même pour les enfants atteints de troubles du développement qui peuvent lutter pour développer des relations hors ligne et une acceptation sociale. Les enfants atteints de troubles cognitifs et de troubles du développement expriment souvent un désir exagéré d'établir des amitiés en ligne. Les enfants atteints de troubles du spectre autistique (TSA) et du syndrome de Williams montrent que la vulnérabilité accrue à la violence hors ligne (et en particulier à la sollicitation sexuelle) des enfants souffrant de troubles du développement se traduit dans l'espace en ligne.[45] Les troubles du développement peuvent fonctionner de plusieurs manières pour accroître les vulnérabilités, à la fois dans l'espace en ligne et hors ligne. Les troubles peuvent servir à accroître la confiance aveugle et un «comportement d'approche sociale accru»,[46] associés à une plus faible capacité à interpréter les signaux de communication et à l'incapacité de prendre des décisions éclairées et calculées sur qui faire confiance, ou qui conduisent à une vulnérabilité sociale accrue. Il existe également des indications que les enfants souffrant d'autres problèmes de santé mentale, en particulier de dépression, ont tendance à rechercher des relations en ligne et peuvent être plus susceptibles de s'engager avec des étrangers.

Les enfants handicapés peuvent également être plus à risque d'avoir une supervision[47] parentale faible ou minimale, un facteur qui a été identifié comme un facteur de risque important d'expériences en ligne négatives,[48] bien que les preuves à ce sujet soient variées. Par exemple, alors que les enfants atteints de certains troubles du développement (en particulier le syndrome de Williams) sont susceptibles d'être plus à risque d'avoir moins de médiation et d'attention parentales[49], les enfants ayant un handicap physique ont tendance à faire l'expérience d'une plus grande implication

39 Baek et al., 2014).
40 Suseg et al, 2008).
41 Mitchell, Ybarra and Korchmaros (2014)
42 Mitchell, Ybarra and Korchmaros (2014)
43 Patchin and Hinduja 2011
44 GLSEN et al., 2013.
45 Lough et al. 2015
46 Lough et al. 2015:4
47 Fisher et al., (2012)
48 Livingstone, (2011)
49 Fisher et al (2012)

parentale, ainsi que d'une plus grande connaissance parentale des activités en ligne de leur enfant.[50] On pourrait supposer que l'attention et l'implication des parents peuvent être corrélées avec la forme de handicap de l'enfant.

Les enfants sont souvent confrontés à l'isolement social résultant de leur statut de minorité et cet isolement est un précurseur de la vulnérabilité. De nombreux enfants cherchent refuge, compagnie ou informations en ligne concernant leur identité sexuelle.

L'un des nombreux avantages qu'offre Internet aux groupes minoritaires est l'utilisation d'espaces en ligne permettant aux enfants et aux jeunes d'explorer leur sexualité. Le soutien qui peut être offert par le biais de forums en ligne et de salons de discussion ou l'accès à des informations sur la santé sexuelle a été largement documenté.[51]

Il est de plus en plus évident que les enfants LGBT sont beaucoup plus susceptibles que les enfants non LGBT de rechercher des informations en ligne sur la santé,[52] les relations amoureuses, la sexualité et la santé sexuelle. De même, l'espace en ligne peut aider à transcender certaines des barrières d'isolement et de communication que les enfants handicapés peuvent rencontrer et offrir plusieurs opportunités[53], notamment sociales ou relationnelles, éducatives ou cognitives. Le fait que cet espace perçu comme sûr et cet environnement favorable soit alors l'espace utilisé pour le harcèlement ou l'intimidation peut exacerber le traumatisme lié au(x) incident(s) d'exclusion, d'intimidation, de harcèlement et d'autres formes de comportements en ligne défavorables.

Dans l'ensemble, la recherche suggère que les enfants vulnérables ou à risque hors ligne sont plus susceptibles d'être également à risque en ligne, aggravant ainsi les cycles de désavantage et de risque. Cela renforce l'argument selon lequel les risques, les préjudices et les vulnérabilités en ligne sont mieux compris dans la littérature et les paradigmes plus larges des risques hors ligne dans la vie des enfants. L'éducation peut réduire les comportements à risque[54] en sensibilisant aux façons dont les choix en ligne (par exemple, le contact avec des étrangers) peuvent augmenter les risques de préjudices, et également en informant les jeunes sur où et comment signaler en toute sécurité des expériences bouleversantes.

2. Droits de l'enfant

Les droits des enfants à accéder à Internet et aux technologies de l'information et de la communication (TIC) sont essentiels à leur développement social et éducatif. Ainsi, restreindre ou refuser les possibilités d'accès à Internet risque de désavantager les enfants. En outre, il existe des preuves substantielles montrant que les compétences numériques jouent un rôle important pour l'apprentissage, la participation et d'autres opportunités des enfants et des jeunes. Les avantages s'appliquent hors ligne et également en ligne, «affectant potentiellement plusieurs dimensions de la vie des enfants dans un monde numérique»[55] . Cependant, le droit à l'accès à Internet augmente également les risques susmentionnés.

50 Whittle et al 2013
51 For examples, see Boyd, 2014; Gray, 2009; Harper et al, 2016; Livingstone, 2017, and Boyd et al. 2011 in relation to self-harm behaviour).
52 GLSEN et al., 2013).
53 SRSG, 2014)
54 Livingstone et al.
55 Haddon, L., Cino, D., Doyle, M-A., Livingstone, S., Mascheroni, G., & Stoilova, M. (2020). Children's and young people's digital skills: a systematic evidence review. KU Leuven, Leuven: ySKILLS p. 8

En outre, certains droits inaliénables inscrits à la fois dans la Convention relative aux droits de l'enfant et dans d'autres traités internationaux que la Tunisie a ratifiés guident les réponses nationales, régionales et internationales. Ceux-ci incluent le droit des enfants à la protection contre les abus et les droits à la justice et à réparation. En réponse à la législation et à la politique face aux risques qui se présentent en ligne, d'autres droits des enfants – le droit à l'éducation, par exemple – ne peuvent être enfreints.

2.1. Droit à la protection contre les abus

En raison de la nature cachée de l'exploitation sexuelle des enfants en ligne et du cadre non réglementé dans lequel elle se déroule, les politiques visant à protéger les enfants utilisateurs des TIC contre l'exploitation sexuelle ne doivent pas être simplement réactives. L'objectif devrait être de prévenir les abus avant qu'ils ne se produisent en renforçant la capacité des enfants à se protéger lorsqu'ils utilisent les TIC. Cette approche est conforme à l'article 19 de la Convention relative aux droits de l'enfant sur le droit à la protection contre les abus, qui souligne l'obligation des États de mettre en œuvre, entre autres mesures, des initiatives éducatives pour protéger les enfants contre toutes les formes de violence [56].

De nombreux parents, écoles et autres autorités optent pour des stratégies d'aversion au risque qui limitent voire interdisent l'accès des enfants aux TIC. «La plupart des parents luttent contre la tension entre protéger leurs enfants et leur donner la liberté d'explorer, d'apprendre et de grandir de manière indépendante» (Livingstone & Byrne 2018 : 27). Le recours à la « médiation restrictive », lorsque les parents ou les tuteurs restreignent le « temps d'écran », interdisent ou supervisent les activités en ligne des enfants, a été une approche. «Dans les pays à revenu intermédiaire et faible, les preuves suggèrent que la médiation restrictive est généralement favorisée par les parents, bien que cela entraîne des coûts en termes d'opportunités pour les enfants en ligne, en particulier pour les filles»[57] . Les parents ou les tuteurs sont également connus pour retirer l'accès à la technologie de l'enfant en supposant qu'aucun accès ne supprimera le risque, la simple restriction de l'accès (à la technologie ou aux sites et services) n'est pas une approche durable ou efficace de la protection.

Cependant, la recherche révèle que restreindre l'accès à Internet n'est pas une approche efficace pour prévenir les risques en ligne[58]. Au lieu de cela, l'éducation (sur la littératie numérique et le sexe, la santé et les relations) est essentielle à cet égard, car les enfants ont besoin d'informations pour se protéger et réagir de manière appropriée aux risques qu'ils peuvent rencontrer en ligne. Cela implique de les sensibiliser aux risques potentiels afin qu'ils puissent les identifier, exercer un jugement critique et faire des choix éclairés. Une prévention efficace des risques dépend en partie des possibilités qu'a l'enfant de développer sa résilience et de pratiquer la citoyenneté numérique.

56 Assemblée Générale des Nations Unies, « Convention relative aux droits de l'enfant »,Pub. L. No. Resolution 44/25 (1989), https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.
57 Livingstone & Byrne (2018) p.19
58 See Kessel, Hardardottir and Tyrefors (2020) https://www.sciencedirect.com/science/article/abs/pii/S0272775719303966?via%-3Dihub

Mais si la sensibilisation et la formation doivent être accessibles aux adultes dans la vie des enfants (parents, tuteurs légaux, enseignants) afin qu'ils connaissent les risques et comment protéger les enfants, cela ne doit pas se substituer à une éducation spécifiquement destinée aux enfants. Notamment, les enfants recherchent en grande partie l'aide ou les connaissances de leurs pairs plutôt que de leurs parents, et il y a eu des évaluations positives des services de mentorat et de soutien par les pairs.

Dans tous les pays, le rythme rapide de l'innovation technologique sape la compétence parentale, ce qui, à son tour, sape la volonté des enfants de se tourner vers leurs parents pour obtenir de l'aide. Nous concluons avec des suggestions pour aider les parents à relever le défi croissant de l'autonomisation de leurs enfants en ligne dans divers contextes.[59]

L'éducation doit être assurée aux enfants d'une manière adaptée à leur âge et à leur sexe. Les ressources de sensibilisation qui encouragent un dialogue constructif et ouvert entre un enfant et un parent ou tuteur légal sont également efficaces. Les TIC et les technologies en ligne devraient également être examinées en tant que facilitateurs de l'exploitation des enfants et, surtout, en tant qu'outil de protection. À cette fin, le Groupe consultatif d'experts indépendants du Secrétaire général des Nations Unies sur une révolution des données pour le développement durable (IEAG)[60] a appelé à l'utilisation de nouvelles technologies pour soutenir les objectifs de développement durable des Nations Unies, dans lesquels l'objectif 16 promeut les efforts visant à mettre fin à la violence et à l'exploitation contre les enfants. Ce sont toutes des considérations importantes dans l'élaboration d'une réponse appropriée à une approche efficace de protection en ligne des enfants.

2.2. Accès à la justice

Lorsque des enfants subissent des violations de leurs droits humains, y compris l'exploitation sexuelle, ils doivent avoir accès à la justice. Le Comité des droits de l'enfant des Nations Unies a déclaré que « pour que les droits aient un sens, des recours efficaces doivent être disponibles pour réparer les violations ». Les États doivent donc « veiller à ce que des procédures efficaces et adaptées aux enfants soient mises à la disposition des enfants et de leurs représentants ». Cela signifie qu'il faut veiller à ce que les enfants aient un accès significatif au système judiciaire - y compris «l'accès à un recours facilement disponible, rapide et efficace sous la forme de procédures pénales, civiles, administratives ou disciplinaires» - et à toute autre procédure de plainte indépendante.

Pour garantir que la sécurité en ligne des enfants devienne une réalité, plusieurs approches différentes mais complémentaires seront probablement nécessaires au niveau national. Cette liste n'est pas exhaustive mais indicative de la complexité de la réponse requise. Idéalement, celles-ci ne devraient pas être conçues isolément des initiatives et approches plus larges (hors ligne) de protection et de sécurité des enfants, mais en relation avec ces questions plus larges :

- Un environnement politique et législatif approprié et réactif;
- Mise en œuvre effective de la législation et des politiques sur le terrain dans les zones urbaines et rurales et dans l'ensemble des systèmes juridiques pluriels;
- Équilibrer les risques et les opportunités : trouver des moyens de promouvoir un engagement sain et sûr tout en protégeant contre les contenus, les contacts et les

59 Livingstone & Byrne (2018) p.19
60 https://www.undatarevolution.org/

comportements potentiellement dangereux[61] ;

- Sensibiliser les parents, les éducateurs et les membres de la communauté à une protection et une prévention efficace;
- Implication des chefs de file de l'industrie en matière de prévention et de consolidation de la sécurité dans la conception ;
- Systèmes de détection et de poursuite efficaces[62] ;
- Systèmes de réponse et de soutien appropriés pour les enfants.

L'Union internationale des télécommunications (UIT) a décrit cinq ensembles de mesures pour promouvoir la sécurité en ligne des enfants. Ces mesures sont également largement reflétées dans le cadre INSPIRE [63] :

- mesures et recours juridiques;
- mesures techniques et procédurales;
- structures organisationnelles ;
- renforcement des capacités ; et
- coopération internationale.

2.3. Protection des données et confidentialité

Les données personnelles sont des informations qui peuvent «identifier ou aider à identifier des personnes directement ou indirectement en combinaison avec d'autres informations»[64] ou «toute information relative à une personne physique identifiée ou identifiable («personne concernée») [65]» . Par conséquent, le traitement des données personnelles [66], à des fins publiques, institutionnelles ou commerciales, est une grave préoccupation pour la confidentialité numérique des individus. La mesure dans laquelle les données personnelles traitées sont exploitées, par les gouvernements à des fins de collecte et de contrôle d'informations ou par les entreprises à des fins commerciales, est une question de protection juridique.

61 Smahel et al., "EU Kids Online: Survey Results from 19 Countries."
62 Il est particulièrement important de s'attaquer à la stigmatisation des victimes d'abus sexuels, en créant un espace sûr dans lequel les enfants peuvent signaler les abus et se sentir en sécurité et recevoir une réponse et une protection positives.
63 The International Telecommunication Union, "The ITU Guidelines on Child Online Protection," May 21, 2021, https://digitalregulation.org.
64 Livingstone, S., Stoilova, M., and Nandagiri, R., (2019) 'Children's data and privacy online: Growing up in a digital age', London School of Economics and Political Science, London. P.49
65 GDPR – Article 4
66 traitement», toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel ou sur des ensembles de données à caractère personnel, par des moyens automatisés ou non, tels que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, la récupération, la consultation, l'utilisation , divulgation par transmission, diffusion ou autre mise à disposition, alignement ou combinaison, restriction, effacement ou destruction (GDPR Article 4)

En particulier, la « datafication des enfants »[67] est un problème important pour la confidentialité et la sécurité en ligne. Le règlement général sur la protection des données (RGPD) de l'Union européenne de 2018[68] reconnaît le droit des enfants à la vie privée. Elle vise à « protéger les enfants et leurs données personnelles dans le monde numérique » et « cherche à rendre une mesure de contrôle à l'individu (ou à l'internaute) concernant sa vie privée en ligne » [69]. Il fait valoir que

> «Les enfants méritent une protection spécifique en ce qui concerne leurs données personnelles, car ils peuvent être moins conscients des risques, des conséquences et des garanties concernés et de leurs droits par rapport au traitement des données personnelles. Cette protection spécifique devrait notamment s'appliquer à l'utilisation des données personnelles des enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateurs et à la collecte de données personnelles concernant les enfants lors de l'utilisation de services proposés directement à un enfant"[70]

L'UNICEF reconnaît que les entreprises commerciales recueillent plus de données sur les enfants que même les gouvernements ne le font ou ne peuvent en recueillir[71], tandis que «les tactiques invasives utilisées par les spécialistes du marketing pour recueillir des informations personnelles sur les enfants ont suscité des inquiétudes en matière de confidentialité et de sécurité des données. »[72] Par conséquent, évaluer si les citoyens tunisiens et les mineurs ont à la fois le droit et le recours effectif à la protection des données personnelles et de la vie privée en ligne est primordial pour développer un PAN efficace.

L'engagement avec le ministère de l'Intérieur et les représentants de l'industrie des TIC aidera à comprendre dans quelle mesure les enfants bénéficient de la confidentialité en ligne[73] et si/ comment leurs données sont utilisées à des fins commerciales.

En plus de la protection contre la vie privée institutionnelle et commerciale, les enfants doivent apprendre à gérer leur «vie privée interpersonnelle» concernant leur communication en ligne ou le partage d'informations. Il s'agit souvent d'un concept relationnel, plutôt que sur une base individuelle[74], et est lié à quelles informations sont partagées, quand et avec qui. Il est important de noter que cette relation «peut être égale ou inégale en termes de pouvoir et de contrôle sur l'utilisation des données personnelles»[75] .

67 La « datafication » fait référence au processus de surveillance et de collecte de données intensifié dans lequel les personnes (y compris les enfants) sont quantifiées et objectivées - positionnées comme des objets (servant les intérêts des autres) plutôt que comme des sujets (ou des agents de leurs propres intérêts et préoccupations); voir Lupton, D. and Williamson, B. (2017) The datafied child: The dataveillance of children and implications for their rights. New Media & Society 19(5), 780-94. From Livingstone, S., Stoilova, M., and Nandagiri, R., (2019) 'Children's data and privacy online: Growing up in a digital age', London School of Economics and Political Science, London.

68 https://gdpr-info.eu/

69 Livingstone, S., Stoilova, M., and Nandagiri, R., (2019)

70 Recital 38 of the GDPR

71 Livingstone, S., Stoilova, M., and Nandagiri, R., (2019) 'Children's data and privacy online: Growing up in a digital age', London School of Economics and Political Science, London.

72 Livingstone, S., Stoilova, M., and Nandagiri, R., (2019) 'Children's data and privacy online: Growing up in a digital age', London School of Economics and Political Science, London.

73 individual control over information disclosure and visibility Ghosh, A.K., Badillo-Urquiola, K., Guha, S., et al. (2018) Safety vs. surveillance: What children have to say about mobile apps for parental control. Conference on Human Factors in Computing Systems. Montreal, Canada: ACM, 1-14.

74 Hargreaves, S. (2017) Relational privacy and tort. William and Mary Journal of Women and the Law 23(3), 433-76.

75 Livingstone, S., Stoilova, M., and Nandagiri, R., (2019) 'Children's data and privacy online: Growing up in a digital age', London School of Economics and Political Science, London. P49

Par conséquent, pour améliorer la protection des données et la confidentialité, la formation et l'éducation à la culture numérique doivent aider les enfants à comprendre «comment les informations sont partagées et peuvent être utilisées en ligne à la fois dans les relations interpersonnelles et dans des contextes commerciaux»[76] afin qu'ils puissent bénéficier d'Internet tout en minimisant les risques[77].

V. Cadres internationaux

Comme indiqué ci-dessus, l'industrie technologique, la technologie numérique et Internet sont de nature mondiale, connectés et dépendants de relations, de contacts et d'environnements couvrant des pays, des régions et le monde. Compte tenu de cela, toute tentative d'élaboration de stratégies ou de politiques visant à assurer la sécurité des enfants en ligne doit être située dans des contextes et des pactes mondiaux, et tenir compte de la fusion des risques hyper-locaux et des dommages potentiels, ainsi que de la nature internationale de nombreuses formes de risques qui les enfants rencontrent en ligne et les préjudices potentiels qui peuvent en résulter.

1. Conventions internationales applicables à la Tunisie

La sécurité et le bien-être des enfants en ligne ne peuvent être dissociés des droits plus larges dont jouissent les enfants. La sécurité des enfants repose sur les droits de tous les enfants, inscrits dans la Convention relative aux droits de l'enfant, à la protection contre les préjudices (article 19) [78] . Il est donc impossible de parler de la protection des enfants contre l'exploitation et les abus sexuels d'enfants en ligne (EASEL) et de toutes les formes de violence facilitées par la technologie, sans parler des droits collectifs et indivisibles des enfants.[79]

L'importance croissante d'Internet et de la technologie dans la vie des enfants, et les opportunités qu'ils présentent, signifient que lorsque nous nous assurons que les enfants sont protégés en ligne, les opportunités que le monde numérique offre aux enfants ne sont pas réduites. Les droits de tous les enfants sont inscrits dans la Convention des Nations Unies relative aux droits de l'enfant (CRC), à laquelle la Tunisie (ainsi que tous les pays sauf deux dans le monde) sont parties[80] . La CDE identifie tous les droits auxquels les enfants ont droit et qui doivent être protégés par les États membres de l'ONU, allant du droit à la vie privée, à la protection et à l'éducation, au droit au logement, à l'éducation et aux soins de santé.

Tout comme les enfants ont le droit d'être en sécurité hors ligne, ils ont le droit à l'éducation, à l'eau, à l'assainissement et aux soins de santé, et ces droits ne doivent pas être compromis par les mesures prises pour assurer la sécurité des enfants. Le droit à l'éducation, par exemple, ne peut se faire au détriment de la sécurité, si les écoles ne sont pas sûres. De même, le droit à l'éducation ne peut être compromis pour garantir le droit d'un enfant à la sécurité et à vivre sans danger. La même chose s'applique en ligne.

76 Livingstone, S., Stoilova, M., and Nandagiri, R., (2019) 'Children's data and privacy online: Growing up in a digital age', London School of Economics and Political Science, London. P49
77 Conseil de l'Europe. (2020) Manuel pour les décideurs politiques sur les droits de l'enfant dans l'environnement numérique : https://rm.coe.int/publication-it-handbook-for-policy-makers-on-the-rights-of-the-child-f/1680a0ae2c
78 Comité des droits de l'enfant des Nations Unies. (1989). Convention relative aux droits de l'enfant. Résolution 44/25 de l'Assemblée générale, 20 novembre 1989.
79 Livingstone, Sonia; Byrne, Jasmina; Carr, John (2016). One in Three: Internet Governance and Children's Rights, Innocenti Discussion Papers, no. 2016-01, UNICEF Office of Research - Innocenti, Florence
80 Comité des droits de l'enfant des Nations Unies. (1989). Convention relative aux droits de l'enfant..

Le droit d'être en sécurité en ligne ne peut pas se faire au détriment des droits à l'éducation, à l'information ou aux soins de santé, par exemple, auxquels les enfants peuvent de plus en plus accéder en ligne. De même, des recherches menées dans le monde entier ont montré que lorsque les enfants ne sont pas en sécurité en ligne, ils ne sont pas en mesure de réaliser pleinement les avantages qui existent pour eux grâce à Internet et à la technologie[81].

L'observation générale .25 exige des États (entre autres) qu'ils prennent des mesures, notamment par l'élaboration, le suivi, la mise en œuvre et l'évaluation de législations, de réglementations et de politiques, pour garantir le respect par les entreprises de leurs obligations d'empêcher l'utilisation de leurs réseaux ou services en ligne dans moyens qui causent ou contribuent à des violations ou des abus des droits des enfants, y compris leurs droits à la vie privée et à la protection, et de fournir aux enfants, aux parents et aux tuteurs des recours rapides et efficaces.

Jusqu'à récemment, le manque de preuves sur ce qui fonctionne pour assurer la sécurité des enfants en ligne a conduit à des approches de la sécurité en ligne qui restreignent l'accès des enfants et des jeunes à la technologie et à Internet. Aujourd'hui, un nombre croissant de recherches et de preuves nous permettent de mieux comprendre comment protéger les opportunités et les droits des enfants en ligne, tout en assurant leur sécurité.

En janvier 2021, la CRC a pris une décision historique dans son adoption de l'Observation générale 25 (GC.25), notant que tous les droits de l'enfant s'appliquent de la même manière en ligne que hors ligne, et qu'il ne devrait y avoir aucune distinction entre l'environnement numérique et hors ligne [82]. Il est important de noter que l'Observation générale fournit également des orientations à tous les États parties à la CDE sur la réalisation des droits de l'enfant dans l'environnement numérique. Ainsi, la nécessité d'équilibrer le droit à la sécurité et à la protection en ligne avec les opportunités qui se présentent est inscrite dans l'interprétation de la Convention relative aux droits de l'enfant. L'OG.25 énonce également quatre principes transversaux qui sont essentiels à la réalisation des droits de l'enfant dans l'environnement numérique : la non-discrimination, l'intérêt supérieur de l'enfant, le droit à la vie, à la survie et au développement ; et le respect des opinions de l'enfant.

Ces principes ont une incidence directe sur tous les aspects des produits et services offerts par l'industrie technologique et le secteur privé :

- ils doivent tenir compte de la manière dont ces produits et services profitent à tous les enfants, y compris les enfants handicapés; ceux qui n'ont peut-être pas les moyens de payer les services et sont donc considérablement désavantagés dans la réalisation d'autres droits, tels que l'éducation; ou ceux qui peuvent vivre dans des zones rurales (pour ne citer que quelques exemples);
- ils doivent toujours se demander si les produits et services, en particulier ceux qui ciblent les enfants, sont susceptibles d'être dans l'intérêt supérieur de l'enfant, ou s'ils peuvent présenter des risques et nuire à l'intérêt supérieur de l'enfant;

81 Voir par exemple, Kardefelt Winther, Daniel; Livingstone, Sonia; Saeed, Marium (2019). Growing up in a connected world, Innocenti Research Report, UNICEF Office of Research - Innocenti, Florence

82 Comité des droits de l'enfant des Nations Unies. (2021). Observation générale n° 25 (2021) sur les droits de l'enfant en relation avec l'environnement numérique. CEC/C/GC/25. 2 mars 2021.

- ils doivent évaluer si les produits ou services qu'ils fournissent compromettent ou menacent la vie, la survie ou le bien-être de l'enfant, ou peuvent avoir un impact substantiel sur son développement (ceci inclut les produits qui peuvent introduire des risques dans la vie des enfants qui peuvent avoir un impact négativement sur les résultats de développement cognitif, sanitaire ou éducatif) [83] ; et
- ils doivent tenir compte de ce que les enfants eux-mêmes pensent, vivent et expriment à propos de leurs expériences des produits et services, car ils sont mieux adaptés pour refléter leurs propres expériences, plutôt que de se voir imposer ces expériences et ces opinions par des adultes.

Enfin, l'OG.25 appelle les États membres - tous ceux qui ont signé et ratifié la Convention relative aux droits de l'enfant, à veiller à ce que le secteur privé fasse preuve de diligence raisonnable quant à l'impact de leurs produits et services sur les droits de l'enfant, et à prendre des mesures pour surveiller, prévenir et agir contre les entreprises et autres qui enfreignent les droits des enfants tels qu'énoncés dans la Convention [84].

Cela impose explicitement la responsabilité à toutes les industries de la technologie et des télécommunications de s'assurer que leurs produits sont sans danger pour les enfants, tout en protégeant tous les droits concurrents de l'enfant. Ceux-ci incluent le droit à la protection contre les préjudices, à l'information, à la participation et à l'éducation, dans et à travers les produits et services qu'ils développent et fournissent. En outre, il incombe à l'État de veiller à ce que cela se produise et de prendre des mesures lorsque les entreprises violent les droits des enfants. Il identifie également le rôle de l'État pour veiller à ce que des mesures de protection des enfants en ligne soient prises dans tous les endroits où les enfants pourraient accéder à Internet, allant des écoles, des cybercafés, d'autres points d'accès publics et dans les foyers. Il attire l'attention sur le rôle du système de protection de l'enfance au sens large, notant que la protection en ligne devrait être intégrée dans la mesure du possible dans un système plus large de protection et de gestion des cas. Notant l'intersection entre les risques en ligne et hors ligne, l'Observation générale appelle également les États à mettre en œuvre des mesures pour aider les parents et les tuteurs à gérer au mieux l'utilisation des appareils et d'Internet par les enfants, ainsi que des mesures parentales plus larges qui favorisent la communication positive, le soutien, l'empathie et d'autres compétences critiques de la vie.

Outre la CDE et les Observations générales ultérieures, la Tunisie est également signataire, sans réserve, du Protocole facultatif à la CDE sur la vente d'enfants, la prostitution et la pornographie mettant en scène des enfants (OPSC). La Tunisie est également le seul État MENA à avoir ratifié la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (en vigueur depuis 2010), connue sous le nom de Convention de Lanzarote, et est également signataire (bien qu'il n'ait pas pleinement adhéré) à la Convention sur la cybercriminalité, plus connue sous le nom de Convention de Budapest.

83 Une opérationnalisation utile des risques, tels que les risques de contenu, de conduite, de contrat et de contact, peut être trouvée ici: Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. https://doi.org/10.21241/ssoar.71817

84 Comité des droits de l'enfant des Nations Unies, 2021

Bien que la Convention de Lanzarote ait été formulée avant la prise de conscience de l'impact potentiel de l'environnement numérique sur les abus et l'exploitation sexuels des enfants, elle reste le premier traité international qui traite des abus sexuels des enfants au sein de la famille et de l'exploitation sexuelle des enfants dans le tourisme et les voyages. Ses dispositions s'étendent également à l'environnement numérique, et il reste l'un des mécanismes mondiaux de protection des enfants les plus importants et juridiquement contraignants. Plus précisément, l'article 18 prévoit la criminalisation et la prévention des abus sexuels sur les enfants, l'article 19 s'applique à la vente d'enfants dans la prostitution enfantine, les articles 20 et 21 traitent de la pornographie enfantine et l'article 23 de la Convention de Lanzarote traite de la sollicitation d'enfants à des fins sexuelles. La Convention de Budapest (en vigueur en 2016) traite directement des abus sexuels et de l'exploitation des enfants en ligne et, par le biais de l'article 9 de la Convention, traite directement de l'interdiction de la pornographie enfantine.[85]

2. Cadres mondiaux pour la sécurité en ligne

Plusieurs cadres, stratégies et orientations existent au niveau mondial pour aider les pays à développer des stratégies de prévention et de réponse pour lutter contre toutes les formes de violence en ligne contre les enfants, ainsi que des orientations plus ciblées sur l'exploitation sexuelle des enfants en ligne. Celles-ci vont des stratégies nationales telles que les stratégies INSPIRE pour mettre fin à la violence contre les enfants (INSPIRE) et le modèle de réponse nationale (MRN), développé par l'Alliance mondiale WeProtect pour lutter contre l'EASEL. Sont liés à ceux-ci, des conseils spécifiques à l'industrie et aux parties prenantes, qui offrent des protocoles et une assistance spécifique aux parties prenantes identifiées, dans le cadre desquels des actions plus détaillées, directement pertinentes pour leur contexte opérationnel, peuvent être formulées par chacune de ces différentes parties prenantes pour prévenir et répondre à toutes les formes de violence en ligne contre les enfants. Des exemples de ceux-ci incluent les directives de l'UIT pour l'industrie/les parents/les écoles sur la protection en ligne des enfants. Cette section décrit dans les grandes lignes chacun d'entre eux pertinents pour l'industrie technologique, et comment ils peuvent être adaptés au contexte tunisien.

85 Notez que les Conventions de Lanzerote et de Budapest ont été formulées avant la reconnaissance de la nécessité de modifier le langage pour mieux refléter la nature abusive de l'utilisation et de la représentation d'enfants dans la pornographie, et donc les textes originaux font toujours référence au terme de pornographie enfantine, plutôt que la terminologie plus récente, suivant les directives de la CRC, de matériel d'exploitation sexuelle d'enfants (MESE).

2.1. Les stratégies INSPIRE : Sept stratégies pour mettre fin à la violence contre les enfants.

Les stratégies INSPIRE sont sept stratégies fondées sur des données probantes pour mettre fin à la violence contre les enfants, élaborées par l'Organisation mondiale de la santé, l'UNICEF et d'autres organismes internationaux. Ces stratégies se concentrent sur sept domaines :

1. la mise en œuvre et l'application des lois,
2. normes et valeurs,
3. environnements sûrs
4. soutien aux parents et aux soignants,
5. revenu et renforcement économique,
6. les services d'intervention et d'assistance, et
7. éducation et compétences de vie.

Essentiellement, les preuves mondiales montrent que l'investissement dans chacun de ces domaines donne des résultats positifs pour la réduction de la violence à l'égard des enfants. Bien que ces stratégies aient été testées et développées pour lutter contre toutes les formes de violence à l'encontre des enfants, sans se concentrer spécifiquement sur la protection en ligne ou la violence subie par les enfants dans l'espace en ligne, elles ont chacune une incidence directe sur les formes de violence subies en ligne et sur les étapes qui peuvent être prises à la fois pour prévenir et répondre à la violence en ligne contre les enfants.

INSPIRE reflète clairement la nécessité d'une réponse intersectorielle et de l'ensemble de la société pour prévenir la violence à l'égard des enfants sous toutes ses formes. Bien que la capacité nationale d'application de la loi et de justice pénale de l'État soit nécessaire, dans le cadre d'un environnement politique et législatif sain, pour enquêter et poursuivre les crimes contre les enfants, le système de protection de l'enfance, l'éducation et la santé, ainsi que les acteurs non étatiques au sein de la société civile , et l'industrie technologique, doivent participer activement à la création d'environnements normatifs non violents, au soutien des parents et des soignants, à la fourniture de services d'intervention et de soutien et à la fourniture d'une éducation complète à la vie et à la santé.

INSPIRE s'est appuyé sur des preuves de l'importance de fournir des environnements physiques sûrs pour les enfants. Cela peut se traduire par la création et la promotion d'environnements numériques sûrs, un résultat pour lequel l'industrie et le gouvernement ont un rôle essentiel à jouer. L'industrie technologique est tenue de fournir et de promouvoir des environnements numériques sûrs pour les enfants - des espaces numériques, des applications, des jeux et des services qui prennent en compte les besoins et les droits des enfants dès le départ, dès la conceptualisation et la conception même du service ou du produit. Cette prise en compte de l'impact potentiel sur les enfants peut être institutionnalisée par l'adoption d'outils tels que les évaluations d'impact sur les droits de l'enfant et les principes de sécurité (et de confidentialité) dès la conception.

Les stratégies INSPIRE sont importantes pour la Tunisie. Il est important que toute mesure visant à lutter contre la violence à l'encontre des enfants tienne compte de toutes les formes de violence en ligne à l'encontre des enfants, notamment compte tenu du continuum et de l'intersection entre la violence en ligne et hors ligne. Inversement, toutes les mesures ou actions prises pour lutter contre la violence en ligne sont fermement ancrées dans la stratégie plus large visant à mettre fin à la violence à l'égard des enfants, afin d'assurer l'intégration des services et des réponses.

Ces actions sont reflétées dans le deuxième cadre mondial de lutte contre la violence en ligne contre les enfants, et plus particulièrement contre les abus et l'exploitation sexuels des enfants en ligne, le modèle de réponse nationale.

2.2. Le modèle de réponse nationale

Le modèle de réponse nationale est un modèle de cadre que les pays peuvent adopter, et par rapport auquel ils peuvent s'évaluer, pour lutter contre la violence en ligne contre les enfants. Bien qu'il ne soit pas basé sur des éléments de preuve spécifiques, il propose différents domaines thématiques ou « capacités» dans lesquels des activités spécifiques aux niveaux national et local peuvent être adaptées pour produire des résultats positifs ciblés pour les enfants. Ceux-ci inclus :

1. Politique et législation
2. Justice pénale
3. Victime
4. Sociétal
5. Industrie
6. Médias et communication

À l'instar des stratégies INSPIRE, le MRN propose un outil permettant aux pays d'aborder la violence en ligne contre les enfants. Le MRN couvre tous les aspects de la société, mais a une capacité spécifique axée sur l'industrie et son rôle dans la prévention et la réponse à la violence en ligne. Plus précisément, la capacité de l'industrie exige que l'industrie technologique d'un pays :

- Agit sur les procédures de notification et de retrait,
- Est dirigé par des protections statutaires qui permettent à l'industrie de signaler pleinement et efficacement le MESE, y compris sa transmission, à l'agence (d'application de la loi) désignée,
- S'engage dans le développement de solutions innovantes pour aider à résoudre les problèmes locaux de la violence en ligne, et
- S'engage dans une responsabilité sociale d'entreprise efficace axée sur l'enfant.

Une dimension importante du MRN est l'accent qu'il met sur le leadership et la coordination efficaces des différents domaines d'intervention individuels impliqués dans la lutte contre la violence et les abus liés aux TIC. Alors qu'auparavant les interventions pour lutter contre la violence et les abus liés aux TIC se concentraient sur les systèmes de réponse et de soutien, par exemple par le biais de

lignes d'assistance téléphonique et d'assistance téléphonique pour signaler les abus et le soutien ciblé aux victimes, etc., le MNR adopte une perspective sociétale plus large. Cela suit une tendance reflétée dans d'autres approches de santé publique vers des stratégies primaires et secondaires pour prévenir ou réduire l'incidence des dommages en ciblant les politiques et les interventions sur les indicateurs de risque connus, en identifiant et en répondant aux problèmes lorsqu'ils surviennent et en minimisant les effets à long terme des méfaits [86] . C'est un domaine dans lequel les gouvernements et le secteur privé de l'industrie technologique se penchent souvent, soutenant des campagnes de sensibilisation et des messages pour les enfants, les parents et les enseignants sur la sécurité en ligne, sensibilisant ainsi la population aux risques potentiels en ligne.

Individuellement, INSPIRE et le MRN abordent des actions spécifiques pour prévenir et répondre aux différents aspects de la violence contre les enfants. Combinés, ils contribuent à un cadre conceptuel global pour les réponses politiques et programmatiques qui s'appuient sur les contributions de tous les acteurs concernés situés dans un cadre écologique approprié et reflètent la complexité des environnements socio-technologiques contemporains.

2.3. Directives mondiales pour l'industrie du numérique

En plus de l'impératif de se conformer aux cadres ci-dessus, il existe plusieurs cadres et directives spécifiques à l'industrie pour aider l'industrie technologique, des entreprises de médias sociaux aux opérateurs mobiles, développeurs, fintech ou créateurs de contenu, à atteindre ces résultats. Cela peut conduire à un équilibre réussi entre le droit des enfants à la protection contre les préjudices en ligne et leur droit à la vie privée, à l'information et à la participation. Il s'agit notamment des directives COP de l'UIT, des droits de l'enfant et des principes d'affaires et des auto-évaluations des droits de l'enfant du Forum mondial de l'enfant.

Lignes directrices de l'UIT sur la protection en ligne des enfants :

L'Union internationale des télécommunications (UIT), en collaboration avec l'UNICEF, a élaboré des lignes directrices spécifiques pour l'industrie technologique (ainsi que pour les enseignants et les parents), adoptant une approche fondée sur les droits de l'enfant, qui fournissent une feuille de route à l'industrie technologique privée pour assurer et promouvoir protection en ligne. Il est important de noter qu'il ne s'agit pas de lignes directrices générales, mais qu'elles sont ciblées sur les besoins et les opérations de l'industrie de la technologie et des télécommunications, ainsi que sur les parents et les enseignants, respectivement.

Ces lignes directrices décrivent cinq domaines spécifiques dans lesquels l'industrie peut protéger et promouvoir les droits de l'enfant afin d'assurer la sécurité et la protection des enfants :

1. Intégrer les droits de l'enfant dans toutes les politiques d'entreprise et processus de gestion appropriés. Cela nécessite d'examiner les politiques et processus internes de chaque entreprise pour s'assurer que l'intérêt supérieur des enfants est au centre des décisions, et que tous les processus internes sont établis pour protéger le bien-être et les droits des enfants, et pour agir en interne et avec responsabilité, lorsque ces droits sont compromis ou violés.

86 Organisation Mondiale de la Santé. (2006). Guide sur la prévention de la matraitance des enfants: Intervenir et produire des données : https://apps.who.int/iris/bitstream/handle/10665/43686/9789242594362_fre.pdf?sequence=1souteni

2. Développer des processus standard pour gérer le matériel d'exploitation sexuelle d'enfants (MESE). Le matériel d'exploitation sexuelle d'enfants est désormais principalement hébergé, transmis, partagé et produit à l'aide de la technologie numérique. Chaque entreprise, quel que soit le service ou les produits qu'elle fournit, doit disposer de politiques et de protocoles internes et externes pour détecter, identifier, renvoyer et supprimer le matériel MESE des réseaux, URL, services ou produits de l'entreprise, ainsi que pour collaborer avec la législation nationale et internationale, l'application de la loi et la société civile dans la lutte contre le MESE.

3. Créez un environnement en ligne plus sûr et adapté à l'âge. Les produits et services fournis par le secteur privé doivent toujours tenir compte des différents risques auxquels les enfants sont confrontés en ligne – contenu, contact, conduite et contrat – et prendre les mesures nécessaires pour créer des produits « faciles à utiliser, sûrs et privés de par leur conception et leur confidentialité » sont adaptés à l'âge de tous les utilisateurs, y compris les enfants [87].

4. Éduquer les enfants, les soignants et les éducateurs sur la sécurité des enfants en ligne et l'utilisation responsable des TIC. Alors que les entreprises jouent un rôle essentiel pour garantir que les expériences en ligne des enfants et leur utilisation de la technologie sont sûres, les parents, les enseignants et les autres adultes responsables dans la vie des enfants jouent également un rôle important dans la promotion des compétences dont les enfants ont besoin pour rester en sécurité, ainsi que comme en prenant des mesures spécifiques adaptées à l'âge. Les entreprises ont donc un rôle important à jouer dans l'éducation et l'autonomisation des parents et des enseignants dans leur rôle d'assurer la sécurité des enfants, dans la façon d'utiliser et quelles sont les limites d'outils tels que les outils de surveillance parentale, et quelle est l'utilisation appropriée de la technologie et les activités en ligne à différents âges et à tous les stades de développement de l'enfant.

5. Promouvoir la technologie numérique comme mode d'augmentation de l'engagement civique. L'article 13 de la Convention relative aux droits de l'enfant consacre le droit des enfants à l'expression et à la participation, par tous les moyens de leur choix. Cela est également reflété dans l'OG.25 qui note les responsabilités des États pour protéger le droit des enfants à la participation et à l'expression, y compris par l'utilisation de la technologie numérique et d'Internet. Il est important que les entreprises veillent à ce que les produits et services qu'elles développent, et les mesures qu'elles prennent pour protéger les enfants en ligne, n'enfreignent pas le droit de ces mêmes enfants de s'exprimer par le biais de la technologie et d'Internet, ou de participer à la richesse de activités et opportunités qu'offre le fait d'être en ligne. Tout aussi important, les entreprises peuvent investir dans la promotion de la participation des enfants, ainsi que des compétences requises pour participer équitablement à la vie civique.

Il est important de noter que les Lignes directrices de l'UIT à l'intention des décideurs sur la protection en ligne des enfants (COP)[88] sont un rapport complet basé sur la Convention relative aux droits de l'enfant et les objectifs de développement durable des Nations Unies.

87 International Telecommunications Industry. (2020). p 8
88 https://www.itu-cop-guidelines.com/policymakers

Cette recherche s'appuie sur les recommandations, les stratégies et les exemples de meilleures pratiques des rapports pour éclairer à la fois la conception de la recherche et le livrable clé de la recherche : un plan d'action national pour la Tunisie.

Le rapport de l'UIT soutient que dans un plan national de COP, les droits des enfants à l'accès à Internet doivent être équilibrés avec 1) des mécanismes de protection, tels que la réglementation de l'industrie, un cadre juridique, la mise en œuvre de la loi et 2) le développement des compétences sous la forme d'une éducation à la sécurité en ligne [89]

> « Les enfants doivent non seulement avoir accès à Internet, mais aussi être protégés contre les dommages en ligne, et posséder les compétences de citoyenneté numérique nécessaires pour gérer les risques et les menaces en ligne » [90].

Le rapport met l'accent sur la nécessité d'une coordination nationale lors de la création de plans de COP et inclut des approches sur la façon de concevoir une stratégie nationale inclusive, « coordonnée et coopérative multipartite ».

> « La protection des enfants et des jeunes est une responsabilité partagée et les décideurs politiques, l'industrie, les parents, les soignants, les éducateurs et les autres parties prenantes doivent assurer un avenir durable où les enfants et les jeunes peuvent s'épanouir et réaliser leur potentiel - en ligne et hors ligne - et où ils peuvent être garanti un environnement numérique sûr dès la conception et autonomisant » [91].

Une stratégie nationale efficace, cependant, doit inclure la contribution des parties prenantes concernées, à savoir « les enfants et leurs parents, soignants et tuteurs », tandis que les responsabilités du secteur privé envers les droits de l'enfant ne doivent pas être négligées[92] . Le rapport souligne la nécessité d'inclure le point de vue des enfants. Il appelle à « des consultations et des dialogues ouverts avec les enfants, pour développer des mesures mieux ciblées et des actions plus efficaces»[93] et veiller à ce que les besoins des groupes vulnérables ne soient pas exclus.

Il souligne l'importance de la réforme juridique, de l'élaboration de nouvelles politiques ou de l'intégration des politiques existantes, car «les normes internationales relatives aux droits de l'homme (telles que la Convention des droits de l'enfant et ses protocoles facultatifs)» [94] doivent être harmonisées avec les lois nationales.

Dans l'ensemble, il présente un plan d'action idéal en tant que processus inclusif avec des rôles et des responsabilités définis pour les principales parties prenantes, à savoir les ministères, les forces de l'ordre, les organisations de services sociaux et de santé, l'industrie des TIC, la société civile, les enfants et leurs parents/tuteurs, et la communauté universitaire et de la recherche.

89 An overview of existing educational frameworks can be found at Cortesi, Sandra, Alexa Hasse, Andres Lombana-Bermudez, Sonia Kim, and Urs Gasser. 2020. Youth and Digital Citizenship+ (Plus): Understanding Skills for a Digital World. Berkman Klein Center for Internet & Society

90 ITU (2020b) Keeping children safe in the digital environment: The importance of protection and empowerment – Policy Brief. P.3

91 ITU (2020b) Keeping children safe in the digital environment: The importance of protection and empowerment – Policy Brief. P.2

92 ITU (2020b) Keeping children safe in the digital environment: The importance of protection and empowerment – Policy Brief. P.3

93 ITU (2020a) Guidelines for policy-makers on Child Online Protection. p. vi

94 ITU (2020b) Keeping children safe in the digital environment: The importance of protection and empowerment – Policy Brief. P.3

En outre, il défend une vision holistique de la réforme dans laquelle des changements de politique devraient être abordés dans les domaines des droits de l'enfant, de la législation, de l'application de la loi, de la réglementation, du suivi et de l'évaluation, de l'industrie des TIC, des rapports, des services sociaux et de l'aide aux victimes, de la collecte de données et de la recherche, de l'éducation, et sensibilisation et capacité nationales[95]

Droits de l'enfant et principes commerciaux du Global Compact

En plus de ce qui précède, des orientations telles que les Principes relatifs aux droits de l'enfant et aux entreprises (CRBP) du Pacte mondial fournissent un cadre utile à la Tunisie pour examiner le rôle et les responsabilités de l'industrie technologique dans la protection des enfants et la garantie que les droits collectifs des enfants sont protégés.

Le CRBP, développé par le Pacte mondial, l'UNICEF et Save the Children, identifie dix principes auxquels les entreprises doivent adhérer pour garantir le respect des droits de l'enfant.

Les entreprises doivent :

1. S'acquitter de leurs responsabilités de respecter les droits de l'enfant et s'engager à soutenir les droits humains des enfants ;
2. Contribuer à l'élimination du travail des enfants dans toutes les activités et pratiques commerciales ;
3. Fournir un travail décent aux jeunes travailleurs, parents et soignants ;
4. Assurer la protection et la sécurité de tous les enfants dans toutes les activités et installations commerciales ;
5. S'assurer que les produits et services sont sûrs et chercher à soutenir les droits des enfants à travers eux ;
6. Utiliser un marketing et une publicité qui respectent et soutiennent les droits de l'enfant ;
7. Respecter et soutenir les droits des enfants en matière d'environnement et d'acquisition et d'utilisation des terrains;
8. Respecter et soutenir les droits des enfants dans les dispositifs de sécurité ;
9. Aider à protéger les enfants touchés par les situations d'urgence ;
10. Renforcer les efforts de la communauté et du gouvernement pour soutenir et protéger les droits des enfants.

95 ITU (2020b) Keeping children safe in the digital environment: The importance of protection and empowerment – Policy Brief. Pp.5-7

Annexe 2: Cartographie du cadre juridique et institutionnel pour la protection de l'enfant en ligne en Tunisie

I. Le cadre juridique pour la protection de l'enfant en ligne en Tunisie

La cartographie du cadre juridique tunisien a démontré l'existence de plusieurs textes législatifs qui traitent la question de la violence en ligne contre les enfants, d'une façon directe ou indirecte. Ces textes abordent la question sous différents angles revêtant un caractère sectoriel. En effet, il n'existe pas actuellement un texte juridique qui traite la question d'une façon holistique liant entre l'enfance et la violence en ligne. Ainsi, les dispositions relatives à la violence contre les enfants en lignes sont éparpillées sur plusieurs textes. Les types de violence faites aux enfants peuvent être classés en deux grandes catégories:

- les atteintes à l'intégrité physique des enfants ;
- les atteintes à leur dignité humaine.
- Les textes juridiques régissant la matière sont comme suit:
- les textes relatifs à la violence contre les enfants (le code pénal, le code de la protection de l'enfance, Loi organique n°58 - 2017 du 22 août 6027 relative à l'élimination de la violence faite aux femmes, La loi organique n°61 de 2016 du 3 août 2016 sur la prévention et la lutte contre la traite des personnes, La loi organique n°26 de 2015 du 7 août 2015 relative à la lutte contre le terrorisme et de prévention du blanchiment d'argent) ;
- les textes relatifs à l'information/communication (La loi n° 1 de 2001 du 15 janvier 2001 portant promulgation du code les télécommunications, la loi n°63 de 2004 du 27 juillet 2004 relative à la protection des données personnelles, le décret-loi n 115 - 2011 du 2 novembre 2011 relatif à la liberté de la presse, Décret-loi n° 2022-54 du 13 septembre 2022, relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication).

1. L'intégrité physique et morale dans la Constitution de 2022

Le législateur tunisien a élevé le droit à la dignité au rang constitutionnel dans l 'article 25 de la nouvelle Constitution de la République tunisienne qui stipule que « l'État protège la dignité de la personne humaine et le caractère sacré du corps, et interdit la torture morale et physique. » Cette protection est attestée par plusieurs législations antérieures. Ainsi, l'article 24 de la Constitution considère que le droit à la vie est un droit sacré et qu'il n'est pas permis d'y porter atteinte sauf dans des cas extrêmes fixés par la loi. » L'article 30 stipule « l'État protège la vie privée, le caractère sacré du domicile et la confidentialité de la correspondance, des communications et des données personnelles. » De même, L'article 38 consacre le droit à l'accès aux réseaux de communication.

2. La cyberviolence et les crimes électroniques dans le code pénal

La notion du crime électronique a été introduite au code pénal pour la première fois en 1999 en vertu de la loi n° 89 du 2 août 1999 modifiant et complétant certaines dispositions du code pénal. Les articles 172, 199 bis et 199 ter consacre désormais le délit d'information et ont incriminé les actes de parjure qui peuvent résulter de l'utilisation des nouvelles technologies de l'information et de la communication.

L'article 206 du Code pénal stipule qu'« il sera puni d'une peine d'emprisonnement de cinq ans toute personne qui aide intentionnellement une autre personne à se suicider.»

L'Article 226 ter (nouveau) stipule que

« Est puni de deux (2) ans d'emprisonnement et d'une amende de cinq (5) mille dinars celui qui commet le harcèlement sexuel.

Est considéré comme harcèlement sexuel toute agression d'autrui par actes ou gestes ou paroles comportant des connotations sexuelles qui portent atteinte à sa dignité ou affectent sa pudeur, et ce, dans le but de l'amener à se soumettre aux désirs sexuels de l'agresseur ou ceux d'autrui, ou en exerçant sur lui une pression dangereuse susceptible d'affaiblir sa capacité à y résister. »

La peine est portée au double, si :

- la victime est un enfant,
- l'auteur est un ascendant ou descendant de la victime, quel qu'en soit le degré,
- l'auteur a une autorité sur la victime ou abuse de l'autorité que lui confèrent ses fonctions,
- l'infraction commise est facilitée par la situation de vulnérabilité apparente de la victime, ou connue par l'auteur.

Le délai de prescription de l'action publique concernant l'infraction de harcèlement sexuel commise contre un enfant court à compter de sa majorité.

Il ressort clairement de cet article que le harcèlement peut être perpétré par d'autres moyens de communication moderne par l'envoi d'images et d'autres moyens afin d'inciter les autres à répondre aux désirs sexuels et leur faire pression.

En outre, l'article 226 bis après sa révision conformément à la loi n°73 de 2004 du 2 août 2004 stipule que :

«Est puni de six mois d'emprisonnement et d'une amende de mille dinars pouvant porter publiquement atteinte aux bonnes mœurs ou à la morale publique par le geste ou la parole ou gène intentionnellement autrui d'une façon qui porte atteinte à la pudeur.»

Est passible des mêmes peines prévues au paragraphe précédent quiconque attire publiquement l'attention sur une occasion de commettre la débauche par des écrits, des enregistrements, des messages audio ou visuels, électroniques ou optiques. »

Ce texte s'applique plus que tout autre à toutes les œuvres pornographiques diffusées via Internet, étant donné que le législateur a explicitement mentionné les moyens électroniques avec lesquelles toute atteinte aux bonnes mœurs est commise, y compris la médiation dans la prostitution et la pornographie diffusés sur le réseau.

D'autres articles du code pénal, dont les articles 232, 233, 234 et 235 sont applicables aux différents types de violence en ligne.

L'article 232 du Code pénal stipule qu'il est considéré comme proxénète et puni d'un emprisonnement d'un à trois ans et d'une amende de cent à cinq cents dinars, celui ou celle :

1. qui, d'une manière quelconque, aide, protège ou assiste sciemment la prostitution d'autrui ou le racolage en vue de la prostitution ;
2. qui, sous une forme quelconque, partage les produits de la prostitution d'autrui ou reçoit des subsides d'une personne se livrant habituellement à la prostitution;
3. qui, vivant sciemment avec une personne se livrant habituellement à la prostitution, ne peut justifier de ressources suffisantes pour lui permettre de subvenir seul à sa propre existence ;
4. qui, embauche, entraîne ou entretient, même avec son consentement, une personne même majeure, en vue de la prostitution, ou la livre à la prostitution ou à la débauche ;
5. qui fait office d'intermédiaire, à un titre quelconque, entre les personnes se livrant à la prostitution ou à la débauche et les individus qui exploitent ou rémunèrent la prostitution ou la débauche d'autrui.

La tentative est punissable. »

Article 233 : « La peine sera d'un emprisonnement de trois à cinq ans et d'une amende de cinq cents à mille dinars dans les cas où :

1. le délit a été commis à l'égard d'un mineur ;
2. le délit a été accompagné de contrainte, d'abus d'autorité ou de dol ;
3. l'auteur du délit est porteur d'une arme apparente ou cachée ;
4. l'auteur du délit est époux, ascendant ou tuteur de la victime ou avait autorité sur elle ou s'il est son serviteur à gages ou s'il est instituteur fonctionnaire ou ministre du culte ou s'il a été aidé par une ou plusieurs personnes. »

Article 234 : « Sous réserve des peines plus fortes prévues par l'article précédent, sera puni d'un à trois ans d'emprisonnement et d'une amende de cent à cinq cents dinars quiconque aura attenté aux mœurs en excitant, favorisant ou facilitant la débauche ou la corruption des mineurs de l'un ou de l'autre sexe. »

Article 235 : « Les peines, prévues aux articles 232, 233 et 234 précédents, seront prononcées alors même que les divers actes qui sont les éléments constitutifs des infractions auraient été accomplis dans des pays différents.

Les coupables des infractions visées aux articles sus-indiqués seront mis, par l'arrêt ou jugement, en état d'interdiction de séjour pendant deux ans au plus. »

3. La loi n°1 de 2001 du 15 janvier 2001 portant promulgation du code les télécommunications

Le législateur a cherché à l'organisation du secteur des télécommunications, et la création d'une instance nationale des télécommunications.

L'article 86 du code de télécommunications dispose qu'« Est puni d'un emprisonnement de un (1) an à deux (2) ans et d'une amende de cent (100) à mille (1000) dinars quiconque sciemment nuit aux tiers ou perturbe leur quiétude à travers les réseaux publics des télécommunications.»

4. La loi organique n°26 de 2015 du 7 août 2015 relative à la lutte contre le terrorisme et de prévention du blanchiment d'argent

Article 5 stipule qu' «est coupable d'infractions terroristes prévues par la présente loi et encourt la moitié des peines y afférentes quiconque :

- incite par tout moyen, à les commettre, dès lors que cet acte engendre, par sa nature ou son contexte, un danger éventuel de leur commission.
- s'est résolu à les commettre, si cette résolution est accompagnée d'un acte préparatoire quelconque en vue de son exécution.

Si la peine encourue est la peine de mort ou l'emprisonnement à vie, elle est remplacée par une peine d'emprisonnement de vingt ans. »

Le développement des systèmes d'information a conduit à l'émergence de nouvelles formes de criminalité organisée y compris le terrorisme électronique, qui dépend de l'utilisation de capacités scientifiques et techniques dans le but d'intimider les autres et leur faire du mal. Les termes dudit article englobe ce genre d'atteinte faite via internet.

5. Le décret-loi n 115 - 2011 du 2 novembre 2011 relatif à la liberté de la presse

Ce décret stipule dans son article 50 que :

«Seront punis, comme complices d'un acte qualifié de délit, selon les définitions prévues par les articles 51 et suivants du présent décret-loi, ceux qui incitent directement un individu ou plusieurs individus à commettre ledit acte[1] , si l'incitation a été suivie d'effet, et ce par voie de discours, de paroles, de menace dans les lieux publics, par voie d'affiches et annonces exposées au public ou par tout moyen d'information audiovisuelle et électronique, la tentative d'infraction est punissable conformément aux dispositions de l'article 59 du Code pénal. »

Cependant, les dispositions pénales incluses dans la loi sur le terrorisme et dans le décret-loi 115 ne sont pas suffisantes pour incriminer l'incitation au meurtre via Internet. Ces textes sont considérés comme des dispositions particulières fixant leur propre champ d'application dans lesdites lois et sont insuffisantes pour lutter contre toutes les autres formes d'incitation au meurtre en ligne. Il est nécessaire de promulguer un texte général incriminant l'incitation au meurtre par Internet. Toutefois, le législateur n'a pas précisé les moyens retenus à cet effet, mais a stipulé que ceux-ci devaient être l'assistance intentionnelle, c'est-à-dire la nécessité d'établir l'élément d'intention criminelle dans ce crime.

Dans ce contexte, il est nécessaire de s'exposer au jeu du « rorqual bleu » ou au « défi baleine Blue » qui est un jeu en ligne composé de défis pendant cinquante jours et dans le dernier défi le jeu demande au joueur de se suicider. Ce jeu a commencé en Russie en 2013 via le réseau social «Vkontakte» et a causé le premier suicide en 2015.

Un jugement d'urgence numéro 54909 a été rendu par le Tribunal de Première Instance de Sousse le 5 mars 2018 qui ordonne à l'Agence tunisienne de l'Internet, en la personne de son représentant légal, de bloquer le jeu «baleine bleu» et le jeu de Mariam de tous les sites internet, des réseaux sociaux et des boutiques d'applications et des liens de téléchargement accessibles sur Internet tunisien.

Il est venu avec le raisonnement du tribunal:

compte tenu de l'article 46 deuxième paragraphe du Code de protection de l'enfance qu'il est considéré comme danger imminent toute action positive ou négative qui menace la vie de l'enfant ou son intégrité physique ou morale d'une manière qui ne peut être remédiée. Et où il ne fait aucun doute que des jeux aussi dangereux ont une atteinte directe au droit de l'enfant à la vie garanti par l'article 22 de la Constitution, l'article 6 de la Convention internationale relative aux droits de l'enfant et l'article 22 du code de la protection de l'enfance qui le protègent de toutes les formes de violence, de maltraitance et d'abus physique, ce qui nécessite une intervention judiciaire urgente pour protéger le droit de l'enfant à la vie et à l'intégrité physique Selon les dispositions de l'article 201 du CPCC, et ce qui est reconnu par la Constitution à l'article 42.

1 Article 51 criminalise l'incitation à "commettre un crime d'homicide, d'atteinte à l'intégrité physique de l'homme, de viol ou de pillage »

Le juge est convoqué au vu de la gravité des deux jeux évoqués et des dégâts de l'utilisation imminente de celui-ci et le danger imminent qui menace les jeunes. Le législateur tunisien n'a pas soumis le code pénal au délit d'incitation au suicide pur et simple, l'article 206 qui incrimine l'acte d'aider les autres à se suicider exprès est incapable d'englober la situation de l'incitation à se suicider via Internet, qui reste une image privée et nécessite la promulgation d'un texte spéciale.

On peut aussi citer le décret-loi 115 relatif à la liberté de la presse et spécifiquement son article 60 qui stipule « sera puni d'une peine d'emprisonnement d'un à trois ans et d'une amende de trois mille à cinq mille dinars, quiconque aura transmis, par quelque moyen que ce soit, intentionnellement, des informations relatives à des délits de viol ou de harcèlement sexuel sur mineur, mentionner le nom de la victime ou divulguer toute information pouvant permettre de la connaître.

Est puni de la même peine quiconque, sciemment, fournit, distribue, exporte, produit, publie, expose, vend ou possède du matériel pédopornographique. »

6. Loi organique n°58 -2017 du 22 août 2017 relative à l'élimination de la violence faite aux femmes

L'article 3 définit la violence à l'égard des femmes comme :

«Toute atteinte physique, morale, sexuelle ou économique à l'égard des femmes, basée sur une discrimination fondée sur le sexe et qui entraîne pour elles, un préjudice, une souffrance ou un dommage corporel, psychologique, sexuel ou économique et comprend également la menace de porter une telle atteinte, la pression ou la privation de droits et libertés, que ce soit dans la vie publique ou privée. »

Le même article définit les types de violence faites aux femmes au sens de cette loi comme suit :

- Violence physique : tout acte nuisible ou de sévices portant atteinte à l'intégrité ou à la sécurité physique de la femme ou à sa vie, tels que les coups, coups de pieds, blessures, poussées, défiguration, brûlures, mutilation de certaines parties du corps, séquestration, torture et homicide,
- Violence morale : toute agression verbale, telle que la diffamation, l'injure, la contrainte, la menace, l'abandon, la privation des droits et des libertés, l'humiliation, la négligence, la raillerie, le rabaissement et autres actes ou paroles portant atteinte à la dignité humaine de la femme ou visant à l'intimider ou la dominer,
- Violence sexuelle : tout acte ou parole dont l'auteur vise à soumettre la femme à ses propres désirs sexuels ou aux désirs sexuels d'autrui, au moyen de la contrainte, du dol, de la pression ou autres moyens, de nature à affaiblir ou porter atteinte à la volonté, et ce, indépendamment de la relation de l'auteur avec la victime,
- Violence politique : tout acte ou pratique fondé sur la discrimination entre les sexes dont l'auteur vise à priver la femme ou l'empêcher d'exercer toute activité politique, partisane, associative ou tout droit ou liberté fondamentale,

- Violence économique : tout acte ou abstention de nature à exploiter les femmes ou les priver des ressources économiques, quel qu'en soit l'origine, tels que la privation des fonds, du salaire ou des revenus, le contrôle des salaires ou revenus et l'interdiction de travailler ou la contrainte à travailler,
- Discrimination à l'égard des femmes : toute distinction, exclusion ou restriction qui a pour effet ou pour but de porter atteinte à la reconnaissance aux femmes, des droits de l'Homme et des libertés, sur la base de l'égalité complète et effective, dans les domaines civil, politique, économique, social et culturel, ou de compromettre cette reconnaissance ou la jouissance ou l'exercice de ces droits par les femmes, quel que soit la couleur, la race, la religion, la pensée, l'âge, la nationalité, les conditions économiques et sociales, l'état civil, l'état de santé, la langue ou le handicap. »

7. La loi organique n°61 de 2016 du 3 août 2016 sur la prévention et la lutte contre la traite des personnes

L'article premier de cette loi stipule que :

« La présente loi vise à prévenir toutes formes d'exploitation auxquelles pourraient être exposées les personnes, notamment, les femmes et les enfants, à lutter contre leur traite, en réprimer les auteurs et protéger et assister les victimes. »

L'Art. 2 de la même loi stipule : « on entend au sens de la présente loi, par les termes suivants :

- La traite des personnes : Est considérée comme traite des personnes, l'attirement, le recrutement, le transport, le transfert, le détournement, le rapatriement, l'hébergement ou l'accueil de personnes, par le recours ou la menace de recours à la force ou aux armes ou à toutes autres formes de contrainte, d'enlèvement, de fraude, de tromperie, d'abus d'autorité ou d'une situation de vulnérabilité ou par l'offre ou l'acceptation de sommes d'argent ou avantages ou dons ou promesses de dons afin d'obtenir le consentement d'une personne ayant autorité sur une autre aux fins d'exploitation, quelle qu'en soit la forme, que cette exploitation soit commise par l'auteur de ces faits ou en vue de mettre cette personne à la disposition d'un tiers.
- La situation de vulnérabilité : Toute situation dans laquelle une personne croit être obligée de se soumettre à l'exploitation résultant notamment du fait que c'est un enfant, de sa situation irrégulière, d'état de grossesse pour la femme, de son état d'extrême nécessité, d'un état de maladie grave ou de dépendance, ou de carence mentale ou physique qui empêche la personne concernée de résister à l'auteur des faits. »

8. Code de la Protection de l'Enfant

Le code prévoit la prévention de l'exploitation de l'enfant, mâle ou femelle sexuellement et la maltraitance habituelle dans ses articles 20 (qui précise les situations de menaces).

L'article 25 stipule qu'est une exploitation sexuelle de l'enfant qu'il soit garçon ou fille, sa soumission à des actes de prostitution soit à titre onéreux ou gratuit directement ou indirectement.

En effet, cet article n'a pas parlé directement d'abus via internet. Néanmoins, l'utilisation du terme « indirectement » signifie que le législateur a laissé la possibilité que cet article s'applique au cas d'abus par internet puisqu'elle constitue une méthode virtuelle et indirecte de communication.

L'article 24 qui stipule le mauvais traitement habituel signifie la soumission de l'enfant à la torture, à des violations répétées de son intégrité physique, ou sa détention, ou l'habitude de le priver de nourriture, ou de commettre tout acte de brutalité qui est susceptible d'affecter l'équilibre affectif ou psychologique de l'enfant. Ainsi, une autre fois le législateur n'a pas mentionné la maltraitance via internet mais l'utilisation du terme « tout acte de brutalité susceptible de… » a laissé la porte ouverte devant la considération d'actes commises par internet comme actes de maltraitance.

Les articles 31 et 32 du code ont instauré l'obligation de signalement auprès du délégué à la protection de l'enfance concernant les cas qui constituent une menace aux enfants. Cette obligation englobe aussi les personnes tenues par le secret professionnel.

9. La loi n°63 de 2004 du 27 juillet 2004 relative à la protection des données personnelles

L'article premier de la loi n° 63 de 2004 du 27Juillet 2004 dispose que « toute personne a droit à la protection des données personnelles relatives à sa vie privée comme l'un des droits fondamentaux garantis par la Constitution et ne peuvent être traitées que dans le cadre de la transparence, de l'honnêteté et du respect de la dignité humaine, conformément aux exigences de la présente loi. »

Cette loi est donc applicable à toutes les personnes, majeures ou mineures. Donc, elle s'applique bien évidemment aux enfants.

L'article 28 a exigé le consentement du tuteur et le juge de la famille en ce qui concerne le traitement des données à caractère personnel relatives aux enfants. L'intérêt supérieur de l'enfant est la condition exigée par la loi pour donner ce genre d'autorisation.

L'article 30 interdit le traitement des données de l'enfants pour des fins publicitaires sans le consentement du tuteur et du juge de la famille. La même procédure est requise pour le cas de transfert de ces données (article 47).

L'Art. 90 de cette loi stipule :

« Est puni d'un an d'emprisonnement et d'une amende de cinq mille dinars, quiconque :

- effectue intentionnellement un traitement des données à caractère personnel sans présenter la déclaration prévue à l'article 7 ou sans l'obtention de l'autorisation prévue aux articles 15 et 69 de la présente loi, ou continue d'effectuer le traitement des données après l'interdiction de traitement ou le retrait de l'autorisation ;
- diffuse les données à caractère personnel relatives à la santé nonobstant l'interdiction de l'Instance mentionnée au deuxième paragraphe de l'article 65 de la présente loi ;
- transfert les données à caractère personnel à l'étranger sans l'autorisation de l'Instance ;
- communique les données à caractère personnel sans le consentement de la personne concernée ou l'accord de l'Instance dans les cas prévus par la présente loi.

En outre, l'article 93 de la Loi énonce qu'«est puni de trois mois d'emprisonnement et d'une amende de trois mille dinars quiconque diffuse intentionnellement des données à caractère personnel, à l'occasion de leur traitement, d'une manière qui nuit à la personne concernée ou à sa vie privée.

La peine est d'un mois d'emprisonnement et d'une amende de mille dinars lorsque la diffusion a été effectuée sans l'intention de nuire.

La personne concernée peut demander au tribunal d'ordonner la publication d'un extrait du jugement dans un ou plusieurs journaux quotidiens, paraissant en Tunisie choisis par la personne concernée. Les frais de publication sont supportés par le condamné.

Les poursuites ne peuvent être déclenchées qu'à la demande de la personne concernée.

Le désistement arrête la poursuite, le procès ou l'exécution de la peine ».

10. Décret-loi n° 2022-54 du 13 septembre 2022, relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication

L'Article premier précise le domaine d'application du texte: "le présent décret-loi vise à fixer les dispositions ayant pour objectif la prévention des infractions se rapportant aux systèmes d'information et de communication et leur répression, ainsi que celles relatives à la collecte des preuves électroniques y afférentes et à soutenir l'effort international dans le domaine, et ce, dans le cadre des accords internationaux, régionaux et bilatéraux ratifiés par la République tunisienne. »

Par contre, l'article 3 insiste que les infractions mentionnées par le décret-loi sont applicables aux dispositions du code pénal ainsi que d'autres textes. L'alinéa 2 prévoit que « les enfants sont soumis au code de la protection de l'enfant. »

L'article 21 énonce qu'il « est puni de cinq ans d'emprisonnement et d'une amende de trente mille dinars, quiconque aura délibérément détourné des données informatiques appartenant à autrui. La tentative est punissable."

Malgré la vocation générale du texte, il a précisé quelques cas d'abus contre les mineurs et ceci dans l'article 26 qui stipule :

« sous réserve des législations spécifiques, est puni d'une peine d'emprisonnement de six ans et une amende de cinquante mille dinars, quiconque produit, affiche, fournit, publie, envoie, obtient ou détient intentionnellement des données informatiques à contenu pornographique montrant un enfant ou une personne ayant l'apparence d'un enfant s'adonnant à des pratiques sexuelles explicites ou suggestives ou en être victime.

Est passible des mêmes peines prévues par le premier alinéa du présent article, quiconque aura utilisé intentionnellement des systèmes d'information pour publier ou diffuser des images ou des séquences vidéo d'agressions physiques ou sexuelles sur autrui ».

Ainsi, le décret-loi a incriminé la détention/l'obtention intentionnelle, la production, la publication et l'envoi des contenus pornographiques ou ceux liés à des pratiques sexuelles concernant des enfants.

Cet examen du cadre juridique révèle que, s'il existe divers textes cloisonnés pouvant être appliqués dans les crimes de cyberviolence à l'égard des enfants, le manque de clarté juridique signifie que l'efficacité des poursuites dépend de la jurisprudence des juges.

II. Le cadre institutionnel pour la protection de l'enfant en ligne en Tunisie

Cette section donne un aperçu des acteurs institutionnels impliqués dans la protection de l'enfance. Notamment, les procédures et les institutions impliquées dans la protection de l'enfance sont les mêmes que celles impliquées dans la protection et lutte contre la violence en ligne à l'égard des enfants.

1. Les services de police et de garde nationale :

1.2. Les unités spécialisées pour enquêter sur les infractions de violence à l'égard des femmes

Selon l'article 24 de la loi organique n° 2017-58 du 11 août 2017, relative à l'élimination de la violence à l'égard des femmes :

« est créée au sein de chaque commissariat de sûreté nationale et de garde nationale, dans tous les gouvernorats, une unité spécialisée pour enquêter sur les infractions de violence à l'égard des femmes conformément aux dispositions de la présente loi. Elle doit comprendre des femmes parmi ses membres. »

Ces brigades ont été créé depuis conformément à cette loi depuis février 2018. Il existe actuellement 70 brigades au niveau de la sécurité nationale, 58 au niveau de la garde nationale et deux brigades centrales. La figure 1 ci-dessous illustre la structure des unités régionales.

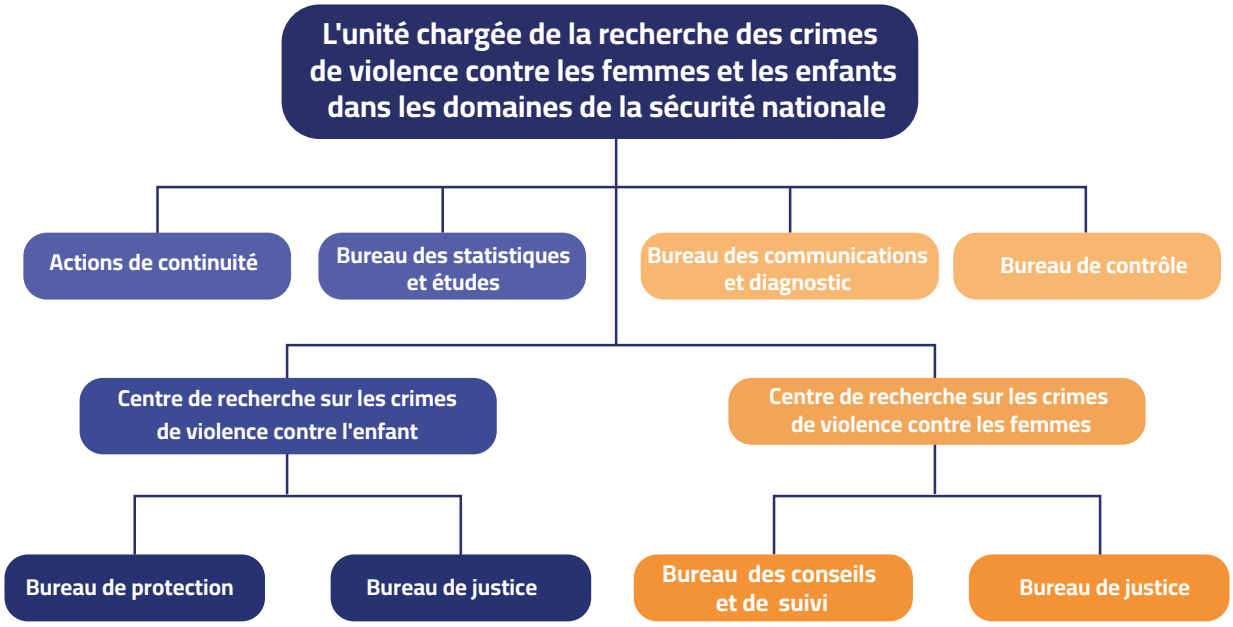

Figure 1: La structure des unités spécialisées pour enquêter sur les infractions de violence à l'égard des femmes et les enfants

Les tâches de ces unités relatives à la protection sont définies à l'article 26 de la même loi, qui stipule :

« L'unité spécialisée peut, sur autorisation du procureur de la République, et avant que l'ordonnance de protection ne soit rendue, prendre l'un des moyens de protection suivants :

- le transfert de la victime et des enfants qui résident avec elle, en cas de nécessité, vers des lieux sécurisés, et ce, en coordination avec les structures compétentes et le délégué à la protection de l'enfance,
- le transfert de la victime pour recevoir les premiers secours lorsqu'elle est atteinte de préjudices corporels,
- éloigner le prévenu du domicile ou lui interdire d'approcher la victime ou de se trouver à proximité de son domicile ou de son lieu de travail, en cas de péril menaçant la victime ou ses enfants qui résident avec elle.

Les procédures de protection continuent à prendre effet jusqu'à ce que l'ordonnance de protection soit rendue. »

1.3. La brigade de la prévention juvénile

C'est une brigade centrale crée en 1966 et organisé par le Décret n° 2007-246 du 15 août 2007, fixant les structures des forces de sûreté intérieure au ministère de l'Intérieur et du Développement Local. Elle est chargée des investigations en relation avec les enfants menacés et les enfants en conflit avec la loi.

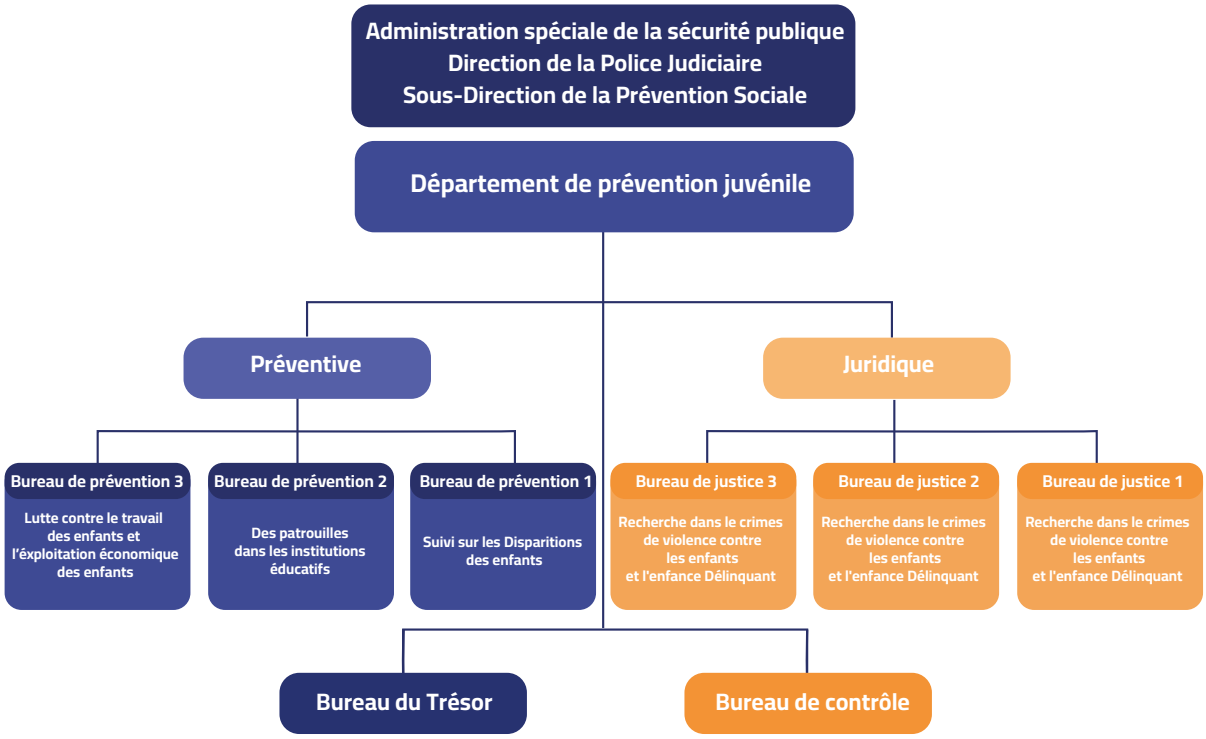

Figure 2: Structure de la brigade de la prévention juvénile

1.4. Brigade de lutte contre la traite des personnes :

Elle a été créée conformément à a loi organique n°61 de 2016 du 3 août 2016 sur la prévention et la lutte contre la traite des personnes. Ses tâches comprennent les investigations sur les infractions liées à la traite des personnes, y compris les enfants.

1.5. La sous-direction de la protection sociale de la Garde nationale

Elle s'engage à enquêter sur les crimes contre les enfants au niveau national. Cette sous-direction assure la coordination avec des unités spécialisées telles que la garde technique et la Police technique et scientifique.

Les unités compétentes sont tenues de rechercher les crimes de violence contre les enfants en coordination avec les déléguées à la protection de l'enfance sur tout le territoire.

Il existe également des unités (centres de recherche sur les crimes de violence contre les enfants dans les unités spécialisées) dans toutes les zones de compétence de la garde nationale.

1.6. La Brigade de lutte contre les délits technologiques

Elle est située à la fois dans la direction générale de la sécurité nationale et dans la direction générale de la garde nationale. Cette brigade s'occupe des investigations dans les crimes sur Internet et les crimes de communication, à la fois contre les enfants et adultes et travaille en contact permanent avec les opérateurs de télécommunications, les fournisseurs d'accès à Internet et l'Agence Tunisienne des Télécommunications.

2. Le délégué à la protection de l'enfance (DPE)

Il est une structure d'intervention préventive dans toutes les situations difficiles qui menacent la santé de l'enfant ou son intégrité physique ou morale, prévues par l'article 20 du code de la protection de l'enfant. Le/la DPE est chargé de coordonner entre les différents acteurs concernés par l'enfance (affaires sociales, de la justice et des droits humains, la santé publique, l'éducation et la formation, le ministère de l'Intérieur et du Développement Local ...), ainsi que les associations et organisations, et en se fondant sur le principe de l'intérêt supérieur de l'enfant.

Les délégués à la protection de l'enfance sont sous la tutelle du ministère chargé de l'enfance et agissent suite à un signalement.

Le signalement est un mécanisme de protection basé sur le fait d'informer le délégué à la protection de l'enfance en cas où on remarque une situation de menace physique ou morale sur un enfant de moins de 18 ans. Selon l'article 31 du code de la protection de l'enfance, le signalement est un devoir pour tout citoyen y compris ceux tenu par le secret professionnel tels que les médecins et les avocats.

Le signalement se fait par tout moyen, direct, téléphonique, lettre ou par voie électronique a travers le site web des délégués à la protection de l'enfance. La loi interdit la divulgation de l'identité de celui qui a fait un signalement et apporte des pénalités pour ceux qui révèlent son identité.

3. Les autorités judiciaires

3.1. Le juge de la famille

C'est un juge du deuxième grade spécialisé dans l'enfance menacé situé au sein des tribunaux de première instance. Selon l'article 58 du code de la protection de l'enfant (CPE) :

- «Le juge de la famille procède à l'audition de l'enfant, ses parents ou la personne qui en a la charge, ou la garde, ou son tuteur.
- Il reçoit les observations du représentant du ministère public, du délégué à la Protection de l'Enfance, et en cas de besoin de l'avocat.
- Il peut décider des plaidoiries sans la présence de l'enfant, pour son intérêt. »

Selon l'article 59 du code,

«le juge de la famille peut prononcer l'une des mesures suivantes:

(l) maintenir l'enfant auprès de sa famille;

(2) maintenir l'enfant auprès de sa famille et charger le délégué à la Protection de l'Enfance du suivi de l'enfant, de l'aide et de l'orientation de la famille;

(3) soumettre l'enfant à un contrôle médical ou psychique;

(4) mettre l'enfant sous régime de tutelle ou le confier à une famille d'accueil ou à une institution sociale ou éducative spécialisée;

(5) placer l'enfant dans un centre de formation ou un établissement scolaire. »

Le législateur a précisé à l'article 51 du CPE les cas de saisine du juge de la famille pour la prise en charge l'enfant menacé, et ce, sur simple demande émanant du juge pour enfants, du ministère public, du délégué à la protection de l'enfance, des services publics d'action sociale et des institutions publiques chargées des affaires de l'enfance. Le juge de la famille peut s'autosaisir lui-même des cas cités dans le CPE.

Il faut noter que le juge de la famille contrôle les interventions du délégué à la protection de l'enfance pendant la phase de la protection sociale.

3.2. Le ministère public

Le ministère public charge le juge de la famille de toute situation difficile mettant un enfant en danger. En tant qu'autorité judiciaire qui contrôle les différentes infractions commises et qui reçoit les plaintes, les notifications et les procès-verbaux transmis par les officiers de la police judiciaire, le ministère public est en mesure d'identifier les situations difficiles auxquelles l'enfant est exposé. En outre, il est la première instance susceptible de prendre connaissance de la situation de l'enfant menacé dans les dossiers d'affaires civiles dans lesquels l'enfant est partie prenante ou lorsque le ministère public est parti dans une affaire impliquant un/e mineur/e à l'instar des actions en contestation de la filiation.

Le ministère public peut également charger le juge de la famille de toute affaire dans laquelle un enfant, dont l'âge est inférieur à 13 ans révolu, a commis une infraction, mais qui est présumé irréfragablement n'avoir pas la capacité d'enfreindre la loi pénale.

3.3. Le juge d'instruction pour enfants

Bien que l'article 51 du CPE n'ait pas prévu la possibilité de saisine du juge de la famille par le juge d'instruction pour enfants, l'article 92 a permis au juge d'instruction de prendre une décision « de non-lieu » et de déférer le dossier au juge de la famille s'il le juge nécessaire dans les situations où il n'y a pas de preuve que l'enfant a commis une infraction punie par la loi, mais où l'enfant semble menacé.

Le juge de la famille peut être saisi sur la base d'un rapport écrit ou verbal du juge d'instruction des enfants ou du juge d'instruction dont l'objet est le signalement d'un cas de menace si ce dernier a constaté cette situation au cours de l'accomplissement de sa fonction (suite à l'audition d'un enfant victime ou témoin).

4. L'instance nationale de la protection des données personnelles (INPDP)

Cette instance a commencé à exercer ses prérogatives en 2009, après désignation de ses membres en 2008. Sa création est inscrite dans la loi organique n°2004-63 relative à la protection des données personnelles, adoptée le 27 juillet 2004, tandis que son fonctionnement a été déterminé ultérieurement par le décret n°2007-3003 du 27 novembre 2007. Sa mission est de veiller au respect des dispositions de la loi relative à la protection des données en mettant en œuvre les moyens nécessaires à l'exercice de son mandat, tels que des manuels de procédures, des formations et des campagnes de sensibilisation.

Article 76 de la loi organique n°2004-63 stipule :

« L'Instance Nationale de Protection des données à Caractère Personnel est chargée de

missions suivantes :

- accorder les autorisations, recevoir les déclarations pour la mise en œuvre du traitement des données à caractère personnel, ou les retirer dans les cas prévus par la présente loi ;
- recevoir les plaintes portées dans le cadre de la compétence qui lui est attribuée en vertu de la présente loi ;
- déterminer les garanties indispensables et les mesures appropriées pour la protection des données à caractère personnel ;
- accéder aux données à caractère personnel faisant l'objet d'un traitement afin de procéder à leur vérification, et collecter les renseignements indispensables à l'exécution de ses missions ;
- donner son avis sur tout sujet en relation avec les dispositions de la présente loi ;
- élaborer des règles de conduite relatives au traitement des données à caractère personnel ;
- participer aux activités de recherche, de formation et d'étude en rapport avec la protection des données à caractère personnel, et d'une manière générale à toute activité ayant un rapport avec son domaine d'intervention ».

Article 77 de la même loi autorise l'instance à

« procéder aux investigations requises en recueillant les déclarations de toute personne dont l'audition est jugée utile et en ordonnant de procéder à des constatations dans les locaux et lieux où a eu lieu le traitement à l'exception des locaux d'habitation. L'Instance peut se faire assister, dans

le cadre de ses missions, par les agents assermentés du ministère chargé des technologies de la communication pour effectuer des recherches et des expertises spécifiques, ou par des experts judiciaires, ou par toute personne jugeant utile sa participation.

L'Instance doit informer le procureur de la République territorialement compétent de toutes les infractions dont elle a eu connaissance dans le cadre de son travail.

Le secret professionnel ne peut être opposé à l'instance. »

5. L'Instance Nationale de Lutte Contre la Traite des Personnes (INLTP)

Cette instance a été créée en vertu de la loi organique n°2016-61 du 3 août 2016 relative à la prévention et la lutte contre la traite des personnes. Les missions de l'instance sont entre autres le développement d'une stratégie nationale de prévention et de lutte contre la traite, ainsi que de la mise en place de mécanismes coordonnés d'identification, de prise en charge et de protection des victimes, de réduction de la demande et aussi de poursuite judiciaire des auteurs. Ainsi, la première stratégie nationale de lutte contre la traite des personnes en Tunisie a été lancée en juillet 2018 pour la période 2018-2023.

6. Coordination avec les institutions éducatives

La coordination est très importante avec cet intervenant, notamment en raison de ses particularités à tous les niveaux.

Le juge doit être attentif aux sensibilités qui peuvent affecter le processus de coordination, surtout si les décisions du juge entrent en conflit avec les orientations de l'établissement d'enseignement. Pour éviter ces problèmes, le juge peut, avant de rendre toute décision affectant le statut scolaire de l'enfant, communiquer directement ou par l'intermédiaire du délégué à la protection de l'enfance avec les délégations régionales de l'éducation, ou demander des rapports et des propositions. Les représentants de l'administration peuvent également être convoqués pour une audience.

Outre la coordination avec l'administration, le juge peut également se coordonner directement ou administrativement avec le psychologue appartenant au service des délégations régionales de l'éducation, et ce dernier peut assister aux audiences, mais sa convocation nécessite le respect des procédures administratives.

7. Portail de signalement des photos et des vidéos d'abus et d'exploitation sexuelle IWF Tunisie

Le portail pour protéger les enfants contre les abus et l'exploitation en ligne a été lancé en 10 juin 2021, par le Ministère de Famille, de la Femme, de l'Enfance et des Seniors de Tunisie et Internet Watch Foundation (IWF), en coopération avec le Partenariat Global 'End Violence against Children, le Conseil de l'Europe dans le cadre du programme conjoint avec l'Union européenne (Programme

Sud IV1), et le Fonds des Nations unies pour l'enfance (UNICEF).

La Tunisie devient ainsi le 47ème pays du monde disposant d'un portail de ce type mis en place par IWF, le 23ème en Afrique et parmi les tout premiers en Afrique du Nord et dans la région MENA.

La propagation sur Internet de matériels d'abus sexuels d'enfants est un phénomène mondial nécessitant à la fois une prise de responsabilité au niveau de chaque pays et une coopération internationale renforcée.

Ce portail de signalement contribue au processus national de prévention et de protection contre les cyberviolences sexuelles à l'encontre des enfants ainsi qu'à la responsabilisation de la société. Il permettra aux citoyens tunisiens de signaler de façon sécurisée et anonyme les images et vidéos d'abus sexuels à l'encontre des enfants diffusés sur Internet en vue de les supprimer.

Lien du portail de signalement en Tunisie : https://report.iwf.org.uk/tn

Annex 3: Indicateurs pour la sélection des sites de recherches

Les sites de recherche ont été déterminé après des consultations et discussions avec le MFFES. Les lieux des groupes de discussion de **Gafsa, Kasserine, Jendouba et du Grand Tunis** ont été sélectionnés sur la base de trois indicateurs importants et interconnectés relatifs à la vulnérabilité des enfants établis en consultation avec le MFFES : les indicateurs de développement régional, le taux de réussite au baccalauréat et le taux d'abandon scolaire. Cela a permis aux groupes de discussion de répondre aux besoins de recherche tout en tenant compte des limites budgétaires et temporelles.

I. Les indicateurs de développement régional

Les disparités régionales, dues à des décennies de politiques de développement inégales en Tunisie, ont conduit à des vulnérabilités accrues auxquelles sont confrontés les enfants des milieux ruraux intérieurs par rapport à leurs pairs des zones urbaines côtières. En effet, il existe des différences concevables dans la connaissance, l'utilisation et la sensibilisation aux TIC et aux risques qui y sont associés, ainsi que dans le signalement entre les enfants vivant dans les zones rurales et urbaines. Cela peut également être un facteur à la fois dans l'utilisation de différentes applications, l'exposition au risque et la relation entre les risques en ligne et hors ligne. Pour quantifier cette disparité, cette recherche utilise l'Indice du Développement Régional développé par l'Institut Tunisien de la Compétitivité et des Études Quantitatives (ITEQ). L'indice révèle des disparités de développement entre les régions côtières et l'intérieur des pays, les gouvernorats de Kasserine, Kairouan et Jendouba se classant systématiquement au plus bas entre 2015 et 2018.[1] L'indice de 2021 révèle également que « les régions intérieures (Kasserine, Kairouan, Jendouba, Sidi Bouzid) occupant les derniers rangs dans la grille du développement régional, elles constituant les zones les plus défavorisées par rapport au reste du pays. » [2]

En Tunisie, les inégalités socio-économiques régionales historiques ont été aggravées par un « fossé numérique » défavorisant les enfants marginalisés des régions intérieures pauvres. Les enfants représentent 29% de la population tunisienne, ils représentent 40% des pauvres du pays. En outre, les enfants vivant dans les régions rurales de l'intérieur courent un risque accru de vivre dans la pauvreté ou l'extrême pauvreté. Cette précarité a été encore exacerbée par le Covid-19, les taux de pauvreté étant passés de 15,2 % à 19,1 % et l'extrême pauvreté de 2,9 % à 3,3 %.[3] La pandémie a mis en évidence les inégalités existantes dans l'accès à la technologie et au haut débit, en particulier en dehors des centres urbains. Cela a un impact à la fois sur l'accès à la technologie et à l'infrastructure technologique, mais aussi sur la littératie numérique des enfants et des jeunes en ligne.

L'inégalité d'accès à des infrastructures et des services éducatifs adéquats, en raison de ces inégalités régionales, a entraîné dans les régions de l'intérieur des taux d'abandon scolaire plus élevés dans le primaire et le secondaire et des taux d'échec au baccalauréat plus élevés.

1 Boussida, S et al. (2019) L'indice du développement régional 2021. L'Institut Tunisien de la Compétitivité et des Études Quantitatives (ITEQ) http://www.itceq.tn/files/developpement-regional/indicateur-de-developpement-regional-2019.pdf
2 Boussida, S et al. (2022) L'indice du développement régional 2021. L'Institut Tunisien de la Compétitivité et des Études Quantitatives (ITEQ) http://www.itceq.tn/files/developpement-regional/indice-dev-regional-2021.pdf
3 Ministère de la Femme, de la Famille, de l'Enfance et des Séniors (2021) Projet de la politique publique intégrée de la prévention et de protection des enfants. p. 4 http://www.femmes.gov.tn/wp-content/uploads/2017/07/Resum%C3%A9- L'inégalité d'accès à des infrastructures et des services éducatifs adéquats, en raison de ces inégalités régionales, a entraîné dans les régions de l'intérieur des taux d'abandon scolaire plus élevés dans le primaire et le secondaire et des taux d'échec au baccalauréat plus élevés.excutif.pdf

II. Taux de réussite au baccalauréat

L'échec à l'examen national le plus important du système éducatif tunisien est un indicateur clé de la marginalisation sociale et économique. En 2021, les régions côtières les plus aisées de Sousse et Monastir ont enregistré des taux de réussite au baccalauréat de 61% et 62,5% respectivement, tandis que Jendouba (35,7%), dans le Nord-Ouest, suivi de Gafsa (37,39%), dans le sud, ont eu les plus faibles taux de réussite au Baccalauréat.[4]

III. Taux d'abandon scolaire

Les recherches sur la probabilité de décrochage scolaire montrent une association significative avec des événements négatifs de la vie - y compris, entre autres, les problèmes physiques et mentaux de l'enfant et les problèmes parentaux. [5],[6], En outre, la recherche montre une interconnexion claire entre le (sous)développement régional d'une part et le décrochage scolaire d'autre part. En effet, « l'échec scolaire touche surtout les régions du Nord-ouest, ainsi la moitié des effectifs scolaires, dans des gouvernorats comme Jendouba et Béja, abandonne les bancs de l'école. Les facteurs responsables de cet échec sont multiples : école éloignée, obligation de rester à domicile, fournitures scolaires très chères… »[7] Kasserine a le taux d'abandon scolaire le plus élevé (2,3 %) en Tunisie.[8]

Ces trois indicateurs sont étroitement liés et doivent être compris comme tels. Les inégalités régionales génèrent et exacerbent à leur tour d'autres vulnérabilités qui peuvent directement exposer les enfants à un plus grand risque de divers types de violence. Les enfants ayant des niveaux inférieurs de littératie numérique peuvent être désavantagés lorsque l'éducation est en ligne, ce qui entraîne des résultats scolaires inferieurs à leurs pairs (en supposant qu'ils peuvent même se connecter), lui-même un facteur de risque de violence. Ces enfants peuvent également être plus vulnérables à certains types de violence qui se produisent à la fois en ligne et hors ligne, comme la radicalisation et l'exploitation sexuelle des enfants en ligne.

4 Bac.org.tn (2021) Bac Tunisie 2021: Taux de réussite par section et par région. https://bac.org.tn/bac-tunisie-2021-taux-de-reussite-par-section-et-par-region/
5 Gubbels, J., van der Put, C.E. & Assink, M. Risk Factors for School Absenteeism and Dropout: A Meta-Analytic Review. J Youth Adolescence 48, 1637–1667 (2019). https://doi.org/10.1007/s10964-019-01072-5
6 Samuel, R., & Burger, K. (2020). Negative life events, self-efficacy, and social support: Risk and protective factors for school dropout intentions and dropout. Journal of Educational Psychology, 112(5), 973–986. https://doi.org/10.1037/edu0000406
7 Daghari, S., and Ben Rabah, I., (2022) Etat des lieux et disparités du système éducatif tunisien. Tunisian Institute of Competitiveness and Quantitative Studies (ITEQ) p.6.
8 Daghari, S., and Ben Rabah, I., (2022) Etat des lieux et disparités du système éducatif tunisien. Tunisian Institute of Competitiveness and Quantitative Studies (ITEQ) p.11

LIGNE VERTE

ASSISTANCE, ORIENTATION ET RAPPORT